IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :

Masato YAMAMICHI et al. :

Serial No. NEW : **Attn: APPLICATION BRANCH**

Filed October 8, 2003 : Attorney Docket No. 2003_1411A

ENCRYPTION APPARATUS, DECRYPTION APPARATUS AND ENCRYPTION SYSTEM

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-296219, filed October 9, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Masato YAMAMICHI et al.

By _____
Michael S. Huppert
Registration No. 40,268
Attorney for Applicants

MSH/kjf
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
October 8, 2003

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年１０月　９日

出願番号
Application Number: 特願２００２－２９６２１９

[ST.10/C]: [ＪＰ２００２－２９６２１９]

出願人
Applicant(s): 松下電器産業株式会社

２００３年　６月　５日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０４３７２２

【書類名】　特許願

【整理番号】　2022540381

【提出日】　平成14年10月 9日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 5/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　山道　将人

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　布田　裕一

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　大森　基司

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　館林　誠

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　暗号システム、送信装置及び受信装置

【特許請求の範囲】

【請求項１】外部から入力された平文を暗号鍵で暗号化した暗号文を受信装置へ送信する送信装置であって、

前記受信装置毎に乱数パラメータを記憶する記憶手段と、

前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、

前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備えることを特徴とする、送信装置。

【請求項２】前記暗号手段は、ＮＴＲＵ暗号方式の暗号アルゴリズムを用いて暗号文を生成することを特徴とする、請求項１に記載の送信装置。

【請求項３】前記制御手段は、期間が経過するにつれて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする、請求項１または請求項２に記載の送信装置。

【請求項４】前記制御手段は、前記暗号手段の暗号化回数に応じて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする、請求項１または請求項２に記載の送信装置。

【請求項５】外部から暗号文を受信し、復号鍵で復号する受信装置であって、

前記暗号文を受信する受信手段と、

前記暗号文を復号して復号文を生成する復号手段と、

前記復号文が正しく得られたかどうかを判別する判別手段と、

前記判別手段の判別結果に応じて前記復号鍵を更新する更新手段とを備えることを特徴とする、受信装置。

【請求項６】外部から入力された平文を暗号化した暗号文を送信する送信装置、及び前記暗号文を受信して復号する受信装置から構成される暗号システムであって、

前記送信装置は、

乱数パラメータを記憶するパラメータ記憶手段と、

前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、

前記暗号文を送信する送信手段と、

前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備え、

前記受信装置は、

前記暗号文を受信する受信手段と、

前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とする、暗号システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、同じ復号鍵を使用し続けると暗号化通信が徐々に復号できなくなっていく暗号システムに関するものである。

【０００２】

【従来の技術】

送信装置と受信装置との間で秘匿通信を実現する方法として、公開鍵暗号を用いた暗号化通信がある。簡単に説明すると、送信装置が、通信内容を受信装置の公開鍵を用いて暗号化して送信し、受信装置は、暗号化された通信内容を受信し、それを自身の秘密鍵を用いて復号して元の通信内容を得る方法である（例えば、非特許文献１参照。）。

【０００３】

この方法を用いる一般的な暗号システムでは、送信装置及び受信装置は、ともに複数存在する。まず、送信装置は、通信先受信装置の公開鍵を取得する。この公開鍵は、通信先受信装置が有する秘密鍵と対になるものでありシステムにおいて公開されている。そして、送信装置は、通信すべきデータを上記のように取得した公開鍵で暗号化して送信する。一方で、受信装置は、上記のように暗号化された通信データを受信する。そして、受信装置は、暗号化された通信データを、自身の有する秘密鍵で復号して元の通信データを得る。

【０００４】

ここで、もしも通信先受信装置の有する秘密鍵が暴露されると、上記の暗号システムは、もはや安全ではなくなる。通信先受信装置の公開鍵で暗号化された通信内容は、暴露された秘密鍵をもつ第三者の受信装置でも復号されてしまうからである。従って、受信装置の有する秘密鍵は、外部に露見しないように厳重に管理する必要がある。

【０００５】

しかしながら、場合によっては、何らかの事故や事件により受信装置の有する秘密鍵が暴露されてしまう可能性がある。従って、上記の暗号システムにおいては、受信装置の有する秘密鍵が暴露された場合、もしくはその疑いがある場合には、暴露された秘密鍵と対になる公開鍵の使用を停止する必要がある。

【０００６】

そのような方法の例として、証明書廃棄リスト（Ｃｅｒｔｉｆｉｃａｔｅ Ｒｅｖｏｃａｔｉｏｎ Ｌｉｓｔ、ＣＲＬ）と呼ばれるデータ構造を使用して、受信装置の有する秘密鍵が暴露された場合に、暴露された秘密鍵と対になる公開鍵の使用を停止する方法が開示されている（例えば、非特許文献２参照。）。

【０００７】

また、他の例として、ＩＥＥＥ（Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃｓ Ｅｎｇｉｎｅｅｒｓ）１３９４規格によるシリアルバス上を伝送されるデジタルコンテンツを保護するＤＴＣＰ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ）規格の中では、ＳＲＭ（Ｓｙｓｔｅｍ Ｒｅｎｅｗａｂｉｌｉｔｙ Ｍｅｓｓａｇｅｓ）を使用して、受信装置の有する秘密鍵が暴露された場合に、当該受信装置の公開鍵の使用を停止するようになっている（例えば、非特許文献３参照。）。

【０００８】

以下に、これらの方法を簡単に説明する。

【０００９】

まず、公開鍵は、それを保有する人や物などの識別情報に関連付けられ、信頼

できる第三者機関によりシリアル番号等が付加された形式に変換される。さらに他者による改ざんを防止するためにその第三者機関のデジタル署名を付加する。これを公開鍵証明書と呼ぶ。そして、第三者機関により発行されるＣＲＬやＳＲＭには、秘密鍵の暴露等の理由で使用を停止すべき公開鍵証明書のシリアル番号が記載されている。よって、ＣＲＬやＳＲＭに記載されたシリアル番号をチェックすることにより、暴露された秘密鍵と対になる公開鍵の使用を停止することができる。

【００１０】

この方法を、送信装置と受信装置の間で暗号化通信を行う暗号システムに応用した場合、まず、送信装置は、通信先受信装置の公開鍵証明書のデジタル署名を確認し、その公開鍵証明書から、公開鍵とシリアル番号を取得し、第三者機関から発行されるＣＲＬやＳＲＭを取得する。そして、送信装置は、取得した公開鍵証明書のシリアル番号がＣＲＬやＳＲＭに記載されていれば、その公開鍵の使用を停止する。このことにより、受信装置の有する秘密鍵が暴露されている場合、暴露された秘密鍵と対になる公開鍵の使用を停止することできる。よって、これにより、送信装置と受信装置の間で安全な暗号化通信を実現することができる。

【００１１】

【非特許文献１】

岡本龍明、山本博資、「現代暗号」、シリーズ／情報科学の数学、産業図書、１９９７

【非特許文献２】

山田信一郎　訳、「ディジタル署名と暗号技術」、株式会社ピアソン・エデュケーション、ｐ．１５９～ｐ．２１４、１９９７

【非特許文献３】

Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｒｅｖｉｓｉｏｎ　１．２　（Ｉｎｆｏｒｍａｔｉｏｎａｌ　Ｖｅｒｓｉｏｎ）、［ｏｎｌｉｎｅ］、２００１年７月１１日、［２００２年９月１３日検索］、インターネット＜ＵＲＬ：　ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ／ｄａｔａ／ｉｎｆｏ＿ｄｔｃｐ＿ｖ１＿１

２＿２００１０７１１．ｐｄｆ＞

【００１２】

【発明が解決しようとする課題】

しかし、ＣＲＬやＳＲＭを用いた上記方法では、以下のような課題がある。

【００１３】

（１）送信装置が最新のＣＲＬやＳＲＭを取得できない場合、受信装置の有する秘密鍵が暴露されていても、送信装置は必ずしも当該受信装置の公開鍵の使用を停止できない。これにより、従来の技術では、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続ける恐れがある。

【００１４】

（２）暗号化通信の安全性確保のためには、鍵を定期的に更新することが望ましい。しかし、従来の技術では、鍵を定期的に更新しなくても受信装置は正常に動作するため、受信装置を扱う人に、鍵の更新を促しにくい。

【００１５】

（３）信頼できる第三者機関によるＣＲＬやＳＲＭが必要である。

【００１６】

以下に、上記問題点（１）、（２）、（３）について詳細を説明する。

【００１７】

まず、ＣＲＬやＳＲＭを用いた上記方法では、送信装置が最新のＣＲＬやＳＲＭを取得できず、受信装置の有する秘密鍵が暴露されていても、当該受信装置の公開鍵の使用を停止できない場合がある。例えば、デジタル化された映画コンテンツデータがＤＶＤなどの記録媒体に記録されるシステムであって、映画コンテンツデータは受信装置に相当するプレーヤ毎の暗号鍵で暗号化されてディスクに記録され、プレーヤはこの暗号鍵に対応する復号鍵を有しており、ディスクに記録されている暗号化映画コンテンツデータを復号して、映画を再生するものであり、さらに特定のプレーヤは不正な機器であって再生を防止する目的で、そのプレーヤの公開鍵のＣＲＬやＳＲＭがＤＶＤ等の記憶媒体に記録されて発行されるような場合である。

【００１８】

いま、ある受信装置の秘密鍵が暴露したことが判明したとする。それ以降は、当該受信装置の公開鍵証明書のシリアル番号が追加記載された最新のＣＲＬやＳＲＭは、ＤＶＤに記録されて発行されるが、それ以前に配布されたＤＶＤには古いＣＲＬやＳＲＭが記録されたままである。結果として、古いＤＶＤを用いていると、古いＣＲＬやＳＲＭしか取得できず、必ずしも当該受信装置の公開鍵の使用を停止する効果が得られない。

【００１９】

また、ＳＲＭを用いるＤＴＣＰ規格では、ＩＥＥＥ１３９４シリアルバスで接続された機器間で、機器が持つ古いＳＲＭは他の機器が持つ新しいＳＲＭに更新されていく。すなわち、この仕組みによって、ＤＶＤ等の記憶媒体から新しいＳＲＭを取得する以外にも、他の機器からも新しいＳＲＭを取得できる。しかしながら、この仕組みを用いても、完全には最新のＳＲＭを取得できる保証は無い。結果として、送信装置は必ずしも当該受信装置の公開鍵の使用を停止する効果が得られない。従って、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続ける恐れがある。

【００２０】

次に、ＣＲＬやＳＲＭを用いた上記方法では、受信装置を扱う人に、自身の公開鍵・秘密鍵の更新を促しにくい。これは、送信装置が、ＣＲＬやＳＲＭにより受信装置の公開鍵の使用を停止するまでは、受信装置は、完全に暗号化通信を復号し続けることが可能であることに起因する。以下にこのことを説明する。

【００２１】

従来の技術では、暴露された秘密鍵と対になる公開鍵の使用を停止するためには、最新のＣＲＬやＳＲＭを第三者機関のサーバ等から取得して、ＣＲＬやＳＲＭに記載されたシリアル番号をチェックしなければならない。しかし、一般に、送信装置を扱う人は、ＣＲＬやＳＲＭのチェックを知らずに暗号化通信を行ったり、あるいはサーバ等から最新のＣＲＬやＳＲＭを取得するのが面倒なために、このチェックを無視して暗号化通信を行ったりすることが多い。これは、送信装置が受信装置の公開鍵を取得していれば、ＣＲＬやＳＲＭのチェックを行わなく

とも、送信装置、受信装置共に正常に動作して、暗号化通信を行うことができるからである。そして、送信装置がＣＲＬやＳＲＭのチェックを行わないで暗号化通信を行うと、鍵を定期的に更新しなくても受信装置が正常に動作するため、受信装置を扱う人は、自身の公開鍵・秘密鍵を更新しようとはしない。なお、公開鍵証明書に有効期限を設け、送信装置が有効期限の切れた公開鍵の使用を停止し、受信装置が鍵を更新しない限り、送信装置から受信装置への暗号化通信を行わないようにする方法もある。しかしながら、この場合も、ＣＲＬやＳＲＭを用いる方法と同様に、送信装置を扱う人は有効期限のチェックを知らずに、あるいはこのチェックを無視して暗号化通信を行うことが多い。この結果、ＣＲＬやＳＲＭを用いる方法と同様に、鍵を定期的に更新しなくても受信装置が正常に動作するため、受信装置を扱う人は、自身の公開鍵・秘密鍵を定期的に更新しようとはしない。

【００２２】

最後に、ＣＲＬやＳＲＭを用いた上記方法では、信頼できる第三者機関によるＣＲＬやＳＲＭが前提となっている。これは、信頼できる第三者機関によるＣＲＬやＳＲＭの存在を仮定しなければならない点が問題点である。

【００２３】

そこで、本発明は上記（１）、（２）、（３）の課題に鑑み、送信装置が暗号化通信を行うに際して、暴露された秘密鍵を不正に用いる第三者の受信装置は、期間が経過すると暗号化通信が復号できなくなる暗号化システム、送信装置又は受信装置を提供し、これにより秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することを第１の目的とする。

【００２４】

また、送信装置が暗号化通信を行うに際して、正規の受信者の受信装置は、同じ秘密鍵を使い続けると、復号に失敗する確率が徐々に増大する暗号システム、送信装置又は受信装置を提供し、これにより受信装置又は受信装置を扱う人に、鍵の更新を促すようにすることを第２の目的とする。

【００２５】

また、送信装置が暗号化通信を行うに際して、第三者機関によるＣＲＬやＳＲＭを必要としない暗号システム、送信装置又は受信装置を提供することを第３の目的とする。

【００２６】

【課題を解決するための手段】

請求項１における発明は、外部から入力された平文を暗号鍵で暗号化した暗号文を受信装置へ送信する送信装置が、前記受信装置毎に乱数パラメータを記憶する記憶手段と、前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備えることを特徴とする。

【００２７】

請求項２における発明は、請求項１に記載の送信装置が、ＮＴＲＵ暗号方式の暗号アルゴリズムを用いて暗号文を生成することを特徴とする。

【００２８】

請求項３における発明は、請求項１または請求項２に記載の送信装置において、前記制御手段が、期間が経過するにつれて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする。

【００２９】

請求項４における発明は、請求項１または請求項２に記載の送信装置において、前記制御手段が、前記暗号手段の暗号化回数に応じて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする。

【００３０】

請求項５における発明は、外部から暗号文を受信し、復号鍵で復号する受信装置が、前記暗号文を受信する受信手段と、前記暗号文を復号して復号文を生成する復号手段と、前記復号文が正しく得られたかどうかを判別する判別手段と、前記判別手段の判別結果に応じて前記復号鍵を更新する更新手段とを備えることを特徴とする。

【００３１】

請求項６における発明は、外部から入力された平文を暗号化した暗号文を送信

する送信装置、及び前記暗号文を受信して復号する受信装置から構成される暗号システムであって、前記送信装置は、乱数パラメータを記憶するパラメータ記憶手段と、前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、前記暗号文を送信する送信手段と、前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備え、前記受信装置は、前記暗号文を受信する受信手段と、前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とする。

【００３２】

【発明の実施の形態】

以下、本発明に係る暗号システムの実施の形態について、図面を用いて説明する。

【００３３】

本発明に係る暗号システムは、公開鍵暗号方式の一例として、ＮＴＲＵ暗号方式を用いる。ＮＴＲＵ暗号方式は、多項式の演算で暗号化と復号化を行う公開鍵暗号方式である。このＮＴＲＵ暗号方式、及びＮＴＲＵ暗号方式の公開鍵、及び秘密鍵の生成方法については、Ｊｅｆｆｅｒｙ Ｈｏｆｆｓｔｅｉｎ, Ｊｉｌｌ Ｐｉｐｈｅｒ, ａｎｄ Ｊｏｓｅｐｈ Ｈ. Ｓｉｌｖｅｒｍａｎ,「ＮＴＲＵ: Ａ ｒｉｎｇ ｂａｓｅｄ ｐｕｂｌｉｃ ｋｅｙ ｃｒｙｐｔｏｓｙｓｔｅｍ」, Ｌｅｃｔｕｒｅ Ｎｏｔｅｓ ｉｎ Ｃｏｍｐｕｔｅｒ Ｓｃｉｅｎｃｅ, １４２３, ｐｐ. ２６７－２８８, Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ, １９９８. に詳しく述べられているので、ここでは詳細な説明を省略するが、以下にＮＴＲＵ暗号方式について簡単に説明する。

【００３４】

ＮＴＲＵ暗号方式は、整数のシステムパラメータ、Ｎ、ｐ、ｑを持つ。上記文献には、システムパラメータの例として、（Ｎ，ｐ，ｑ）＝（１０７，３，６４）、（Ｎ，ｐ，ｑ）＝（１６７，３，１２８）、（Ｎ，ｐ，ｑ）＝（５０３，３，２５６）の３つの例が挙げられている。

【００３５】

以降、本発明に係る暗号システムの実施の形態では、システムパラメータＮを

Ｎ＝１６７とした場合の説明を行う。

【００３６】

ＮＴＲＵ暗号方式は、多項式の演算により暗号化と復号化を行う公開鍵暗号方式である。まず、ＮＴＲＵ暗号方式で扱う多項式は、上記システムパラメータＮに対し、Ｎ－１次元以下の多項式であり、例えばＮ＝５のとき、Ｘ＾４＋Ｘ＾３＋１等の多項式である。ここで、「Ｘ＾ａ」はＸのａ乗を意味することとする。また、暗号化時あるいは復号化時に用いる、公開鍵ｈ、秘密鍵ｆ、平文ｍ、乱数ｒ、暗号文ｃはいずれも、Ｎ－１次元以下の多項式として表現される（以降、それぞれを公開鍵多項式ｈ、秘密鍵多項式ｆ、平文多項式ｍ、乱数多項式ｒ、暗号文多項式ｃと呼ぶ）。

【００３７】

そして、多項式演算は、上記システムパラメータＮに対し、Ｘ＾Ｎ＝１という関係式を用いて、演算結果が常にＮ－１次元以下の多項式になるように演算される。例えば、Ｎ＝５の場合、多項式Ｘ＾４＋Ｘ＾２＋１と多項式Ｘ＾３＋Ｘの積は、多項式と多項式の積を×、整数と多項式の積を・とすると、Ｘ＾５＝１という関係から、

（Ｘ＾４＋Ｘ＾２＋１）×（Ｘ＾３＋Ｘ）

＝Ｘ＾７＋２・Ｘ＾５＋２・Ｘ＾３＋Ｘ

＝Ｘ＾２×１＋２・１＋２・Ｘ＾３＋Ｘ

＝２・Ｘ＾３＋Ｘ＾２＋Ｘ＋２

というように、常にＮ－１次元以下の多項式になるように演算される。

【００３８】

暗号化時には、以下に述べる乱数多項式ｒと公開鍵多項式ｈとを用いて、平文多項式ｍに多項式演算である暗号化アルゴリズムＥを施して、暗号文多項式ｃ＝Ｅ（ｍ，ｒ，ｈ）を生成する。ここで、Ｅ（ｍ，ｒ，ｈ）は、ＮＴＲＵ暗号方式の暗号化アルゴリズムＥに、平文多項式ｍ、乱数多項式ｒ及び公開鍵多項式ｈを入力して得られる多項式演算の結果である。暗号化アルゴリズムＥについては上記文献に詳しく述べられており、ここでは説明を省略する。

【００３９】

なお、ＮＴＲＵ暗号方式では、乱数多項式ｒを生成するためのパラメータｄが予め決められており、乱数多項式ｒは、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつ他の係数は０となるように選ぶ。すなわち、乱数多項式ｒはＮ－１次元以下の多項式であり、０次元（定数項）からＮ－１次元まで、Ｎ個の係数があるが、このＮ個の係数のうち、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつ（Ｎ－２ｄ）個の係数は０となるように選ぶ。上記文献によれば、パラメータＮがＮ＝１６７の場合、ｄ＝１８である。すなわち、１８個の係数が１であり、かつ１８個の係数が－１であり、１３１（＝１６７－３６）個の係数が０となるように乱数多項式ｒを選ぶ。

【００４０】

復号化時には、秘密鍵多項式ｆを用いて、暗号文多項式ｃに多項式演算である復号アルゴリズムＤを施して、復号文多項式ｍ’＝Ｄ（ｃ，ｆ）を生成する。ここで、Ｄ（ｃ，ｆ）は、ＮＴＲＵ暗号方式の復号アルゴリズムＤに、暗号文多項式ｃ、及び秘密鍵多項式ｆを入力して得られる多項式演算の結果である。復号アルゴリズムＤについては上記文献に詳しく述べられており、ここでは説明を省略する。

【００４１】

ところで、このＮＴＲＵ暗号方式は、復号文多項式ｍ’が平文多項式ｍと異なる場合が発生する。この場合は、復号時に正しく平文多項式ｍが得られないことになる。このことを復号エラーが発生するという。復号エラーは、乱数多項式ｒ、平文多項式ｍ、公開鍵多項式ｈ、秘密鍵多項式ｆの組み合わせにより、発生するかどうかが決まる。具体的には、公開鍵多項式ｈは、秘密鍵多項式ｆとランダム多項式ｇとの演算結果により生成されるが、この公開鍵多項式ｈを生成したときに用いたランダム多項式ｇ、乱数多項式ｒ、平文多項式ｍ、秘密鍵多項式ｆの演算結果の多項式（ｐ・ｒ×ｇ＋ｆ×ｍ）の係数の値が－ｑ／２からｑ／２の間に入らなかったとき、復号エラーが発生する。この復号エラーの発生を完全に避ける手法は現在知られていないが、上記文献によれば、Ｎ＝１６７の場合、ｄ＝１８とすれば、確率的にほとんど復号エラーは発生せず、実用上問題ないことが明記されている。

【００４２】

（実施の形態１）

本発明の実施の形態１における暗号システム１の全体構成を図１に示す。この暗号システム１は平文多項式ｍの暗号化通信を行うシステムであり、送信装置１１０と複数の受信装置１２０ａ、１２０ｂ、１２０ｃとから構成され、送信装置１１０と受信装置１２０ａ、１２０ｂ、１２０ｃとは通信路１３０を介して接続されている。

【００４３】

以下に、送信装置１１０は複数の受信装置のうち受信装置１２０ａと暗号化通信を行うとし、これらの構成要素について詳細に説明を行う。

【００４４】

送信装置１１０は、図２に示すように、平文入力部１１１、パラメータ記憶部１１２、タイマ部１１３、パラメータ制御部１１４、乱数生成部１１５、暗号化部１１６、送信部１１７及び鍵更新部１１８から構成される。

【００４５】

平文入力部１１１は、外部より入力された平文多項式ｍを暗号化部１１６に出力する。

【００４６】

パラメータ記憶部１１２は、図３に示すように、受信装置１２０ａの固有番号ＩＤａ、公開鍵多項式ｈａ及び乱数パラメータｄａを、一組のデータＤＴａ＝（ＩＤａ，ｈａ，ｄａ）として記憶している（受信装置１２０ｂ、１２０ｃについても同様にＤＴｂ＝（ＩＤｂ，ｈｂ，ｄｂ）、ＤＴｃ＝（ＩＤｃ，ｈｃ，ｄｃ）を記憶している）。ここで、乱数パラメータｄａは、暗号化時に用いる乱数多項式ｒを生成するためのパラメータであり、乱数多項式ｒの係数のうち、係数が１であるものの数、及び係数が－１であるものの数である。なお、乱数パラメータｄａの初期値は、ｄａ＝１８とする。

【００４７】

タイマ部１１３は、一日毎に時間信号を発生し、パラメータ制御部１１４に入力する。

【００４８】

パラメータ制御部１１４は、タイマ部１１３から時間信号を受け取ったら、パラメータ記憶部１１２に記憶された乱数パラメータｄａの値を１ずつ増加させる（乱数パラメータｄｂ、ｄｃの値も、同様に１ずつ増加させる）。

【００４９】

乱数生成部１１５は、パラメータ記憶部１１２から受信装置１２０ａの乱数パラメータｄａを読み出す。そして、読み出した乱数パラメータｄａに基づき、ｄａ個の係数が１であり、かつｄａ個の係数が－１であり、かつその他の係数が０となる乱数多項式ｒをランダムに生成する。そして、生成した乱数多項式ｒを暗号化部１１６へ出力する。

【００５０】

暗号化部１１６は、予めＮＴＲＵ暗号方式の暗号アルゴリズムＥを有している。

【００５１】

暗号化部１１６は、平文入力部１１１から平文多項式ｍを受け取り、パラメータ記憶部１１２から受信装置１２０ａの公開鍵多項式ｈａを読み出し、乱数生成部１１５から乱数多項式ｒを受け取る。そして、暗号化部１１６は、乱数多項式ｒと公開鍵多項式ｈａを用いて、平文多項式ｍに前記暗号アルゴリズムＥを施して暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を生成し、生成した暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を送信部１１７へ出力する。

【００５２】

送信部１１７は、暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を、通信路１３０を介して受信装置１２０ａへ送信する。

【００５３】

鍵更新部１１８は、通信路１３０を介して受信装置１２０ａ、１２０ｂ、１２０ｃから、固有番号と新たな公開鍵多項式を受信することができる。もしも、受信装置１２０ａの固有番号ＩＤａと公開鍵多項式ｈａ’を受信した場合、鍵更新部１１８は、パラメータ記憶部１１２に記憶されているＤＴａ＝（ＩＤａ，ｈａ，ｄａ）を、ＤＴａ’＝（ＩＤａ，ｈａ’，ｄａ’）に更新する。ここでｄａ’

は、乱数パラメータの初期値でありｄａ’＝１８である（受信装置１２０ｂ、１２０ｃから受信した場合は、それぞれ、ＤＴｂをＤＴｂ’、ＤＴｃをＤＴｃ’に更新する）。

【００５４】

以上に述べた送信装置１１０は、以下に述べる暗号化通信処理、乱数パラメータ更新処理及び公開鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

【００５５】

以下に、送信装置１１０の動作について、暗号化通信処理、乱数パラメータ更新処理、公開鍵更新処理に分けて説明を行う。

【００５６】

最初に、送信装置１１０の暗号化通信処理について、図４に示すフローチャートを用いて説明する。

【００５７】

まず、乱数生成部１１５は、パラメータ記憶部１１２から受信装置１２０ａの乱数パラメータｄａを読み出し（ステップＳ１０１）、そして、読み出した乱数パラメータｄａに基づき、ｄａ個の係数が１であり、かつｄａ個の係数が－１であり、かつその他の係数が０となる乱数多項式ｒをランダムに生成し、生成した乱数多項式ｒを暗号化部１１６へ出力する（ステップＳ１０２）。

【００５８】

次に、暗号化部１１６は、平文入力部１１１から平文多項式ｍを受け取り、パラメータ記憶部１１２から受信装置１２０ａの公開鍵多項式ｈａを読み出し、乱数生成部１１５から乱数多項式ｒを受け取り（ステップＳ１０３）、そして、暗号化部１１６は、乱数多項式ｒと公開鍵多項式ｈａを用いて、平文多項式ｍに暗号アルゴリズムＥを施して暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を生成し、生成した暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を送信部１１７へ出力する（ステップＳ１０４）。

【００５９】

次に、送信部１１７は、受け取った暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を、通信

路１３０を介して受信装置１２０ａへ送信して処理を終了する（ステップＳ１０５）。

【００６０】

次に、送信装置１１０の乱数パラメータ更新処理について、図５に示すフローチャートを用いて説明する。

【００６１】

まず、パラメータ制御部１１４は、タイマ部１１３から時間信号を受け取ったら、ステップＳ１１２へ処理を移し、そうでなければ処理を終了する（ステップＳ１１１）。

【００６２】

そして、パラメータ制御部１１４は、パラメータ記憶部１１２に記憶された乱数パラメータｄａの値を１ずつ増加させて（乱数パラメータｄｂ、ｄｃの値も、同様に１ずつ増加させる）、処理を終了する（ステップＳ１１２）。

【００６３】

次に、送信装置１１０の公開鍵更新処理について、図６に示すフローチャートを用いて説明する。

【００６４】

まず、鍵更新部１１８は、受信装置１２０ａ、１２０ｂ、１２０ｃのいずれかから、固有番号と新たな公開鍵を受信したら、ステップＳ１２２へ処理を移し、そうでなければ処理を終了する（ステップＳ１２１）。

【００６５】

そして、鍵更新部１１８は、パラメータ記憶部１１２に記憶されているＤＴａ＝（ＩＤａ，ｈａ，ｄａ）を、ＤＴａ’＝（ＩＤａ，ｈａ’，ｄａ’）に更新して処理を終了する（受信装置１２０ａから受信した場合。受信装置１２０ｂ、１２０ｃから受信した場合は、それぞれ、ＤＴｂをＤＴｂ’、ＤＴｃをＤＴｃ’に更新する）。ここでｄａ’は、乱数パラメータの初期値でありｄａ’＝１８である（ステップＳ１２２）。

【００６６】

受信装置１２０ａは、図７に示すように、受信部１２１、秘密鍵記憶部１２２

、復号化部１２３、復号文出力部１２４、鍵再生成部１２５、及び入力部１２６から構成される。

【００６７】

受信部１２１は、送信装置１１０から通信路１３０を介して、暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を受信し、受信した暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を復号化部１２３へ出力する。

【００６８】

秘密鍵記憶部１２２は、受信装置１２０ａの秘密鍵多項式ｆａを記憶している。

【００６９】

復号化部１２３は、暗号化部１１６が有する暗号アルゴリズムＥの逆変換である、ＮＴＲＵ暗号方式の復号アルゴリズムＤを予め有している。

【００７０】

復号化部１２３は、受信部１２１から暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を受け取り、秘密鍵記憶部１２２から受信装置１２０ａの秘密鍵多項式ｆａを読み出す。そして、復号化部１２３は、秘密鍵多項式ｆａを用いて、暗号文多項式Ｅ（ｍ，ｒ，ｈａ）に前記復号アルゴリズムＤを施して復号文多項式ｍ’＝Ｄ（Ｅ（ｍ，ｒ，ｈａ），ｆａ）を生成し、生成した復号文多項式ｍ’を復号文出力部１２４へ出力する。

【００７１】

復号文出力部１２４は、復号化部１２３から復号文多項式ｍ’を受け取り、復号文多項式ｍ’を外部へ出力する。

【００７２】

鍵再生成部１２５は、入力部１２６を介して鍵再生成要求信号を受け取った場合、ＮＴＲＵ暗号の秘密鍵多項式ｆａ’及び公開鍵多項式ｈａ’を新たに再生成して、秘密鍵記憶部１２２に記憶されている秘密鍵多項式ｆａを新たに生成した秘密鍵多項式ｆａ’に更新する。そして、受信装置１２０ａの固有番号ＩＤａと新たな公開鍵多項式ｈａ’を、通信路１３０を介して送信装置１１０に送信する。

【００７３】

受信装置１２０ａを扱うユーザは、受信装置１２０ａの公開鍵多項式ｈａと秘密鍵多項式ｆａの再生成を指示する鍵再生成要求信号を入力部１２６に入力することができる。この鍵再生成要求信号は、復号文出力部１２４から出力された復号文多項式m’が正しく得られない等の理由で、ユーザが公開鍵多項式ｈａと秘密鍵多項式ｆａの再生成のために入力する信号である。

【００７４】

入力部１２６は、外部から入力された鍵再生成要求信号を鍵再生成部１２５に出力する。

【００７５】

以上に述べた受信装置１２０ａは、以下に述べる復号化処理及び鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

【００７６】

以下に、送信装置１２０ａの動作について、復号化処理、鍵更新処理に分けて説明を行う。

【００７７】

最初に、受信装置１２０ａの復号化処理について、図８に示すフローチャートを用いて説明する。

【００７８】

まず、受信部１２１は、送信装置１１０から通信路１３０を介して、暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を受信し、受信した暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を復号化部１２３へ出力する（ステップＳ１５１）。

【００７９】

次に、復号化部１２３は、受信部１２１から暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を受け取り、秘密鍵記憶部１２２から受信装置１２０ａの秘密鍵多項式ｆａを読み出し（ステップＳ１５２）、そして、復号化部１２３は、秘密鍵多項式ｆａを用いて、暗号文多項式Ｅ（ｍ，ｒ，ｈａ）に復号アルゴリズムＤを施して復号文多項式m’＝Ｄ（Ｅ（ｍ，ｒ，ｈａ），ｆａ）を生成し、生成した復号文多項式m’を復号文出力部１２４へ出力する（ステップＳ１５３）。

【００８０】

次に、復号文出力部１２４は、復号化部１２３から復号文多項式m’を受け取り、復号文多項式m’を外部へ出力して処理を終了する（ステップＳ１５４）。

【００８１】

次に、受信装置１２０ａの鍵更新処理について、図９に示すフローチャートを用いて説明する。

【００８２】

まず、鍵再生成部１２５は、もしも、入力部１２６を介して鍵再生成要求信号を受け取ったら、ステップＳ１６２へ処理を移し、そうでなければ処理を終了する（ステップＳ１６１）。

【００８３】

そして、鍵再生成部１２５は、ＮＴＲＵ暗号の秘密鍵多項式ｆａ’及び公開鍵多項式ｈａ’を新たに再生成して、秘密鍵記憶部１２２に記憶されている秘密鍵多項式ｆａを新たに生成した秘密鍵多項式ｆａ’に更新し（ステップＳ１６２）、受信装置１２０ａの固有番号ＩＤａと新たな公開鍵多項式ｈａ’を、通信路１３０を介して送信装置１１０に送信して処理を終了する（ステップＳ１６３）。

【００８４】

以下に、実施の形態１における暗号システム１全体の動作について説明する。

【００８５】

今、暗号システム１において、送信装置１１０は複数の受信装置のうち受信装置１２０ａと暗号化通信を行うとする。

【００８６】

まず、送信装置１１０は、受信装置１２０ａの固有番号ＩＤａ、公開鍵多項式ｈａ及び乱数パラメータｄａを、データＤＴａ＝（ＩＤａ，ｈａ，ｄｂ）としてパラメータ記憶部１１２に記憶している（受信装置１２０ｂ、１２０ｃについても同様にＤＴｂ＝（ＩＤｂ，ｈｂ，ｄｂ）、ＤＴｃ＝（ＩＤｃ，ｈｃ，ｄｃ）を記憶している）。乱数パラメータｄａ、ｄｂ、ｄｃの初期値は、ｄａ＝ｄｂ＝ｄｃ＝１８である。

【００８７】

そして、送信装置１１０は暗号化通信処理に従って、平文多項式ｍを暗号化して暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を生成し、生成した暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を通信路１３０を介して受信装置１２０ａに送信する。一方、受信装置１２０ａは前述した復号化処理に従って、暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を通信路１３０を介して送信装置１１０から受信し、受信した暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を復号して復号文多項式ｍ’を出力する。

【００８８】

なお、送信装置１１０では、乱数パラメータ更新処理に従って、タイマ部１１３が一日毎に発生する時間信号に応じて、パラメータ制御部１１４は、パラメータ記憶部１１２に記憶された全ての乱数パラメータｄａ、ｄｂ、ｄｃの値を１ずつ増加させる。すなわち、パラメータ記憶部１１２に記憶された全ての乱数パラメータの値は一日毎に増加する。

【００８９】

従って、この送信装置１１０の暗号化通信処理が継続して行われると、暗号文多項式Ｅ（ｍ，ｒ，ｈａ）を生成される際に用いられる乱数多項式ｒは、係数が１であるもの、及び係数が－１であるものの数が一日毎に増加する。

【００９０】

今、図１０は、乱数パラメータｄの値に対し、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつその他の係数が０となる乱数多項式ｒを用いた場合の、ＮＴＲＵ暗号方式の復号エラー発生確率の測定結果である。この測定結果によれば、乱数パラメータｄａの初期値ｄａ＝１８においては、送信装置１１０が生成する暗号文多項式Ｅ（ｍ，ｒ，ｈａ）は、ほとんど復号エラーは発生しない（受信装置１２０は受信した暗号文多項式Ｅ（ｍ，ｒ，ｈａ）から、平文多項式ｍと等しい復号文多項式ｍ’を得ることができる）。一方で、期間が経過すれば、乱数パラメータｄａが一日毎に徐々に大きくなるので、送信装置１１０が生成する暗号文多項式Ｅ（ｍ，ｒ，ｈａ）は、徐々に復号エラー発生確率が大きくなる（受信装置１２０は受信した暗号文多項式Ｅ（ｍ，ｒ，ｈａ）から、平文多項式ｍと等しい復号文多項式ｍ’を得ることが徐々にできなくなる）。

【００９１】

そして、もしも受信装置１２０が平文多項式ｍと等しい復号文多項式ｍ’を得る確率が下がり、実用的な暗号化通信を行うことができなくなった場合、受信装置１２０ａを扱うユーザは、鍵更新処理を行うことにより、受信装置１２０ａの公開鍵多項式ｈａと秘密鍵多項式ｆａの再生成を指示する鍵再生成要求信号を入力部１２６に入力することができる。すると、送信装置１１０の公開鍵更新処理により、パラメータ記憶部１１２の乱数パラメータｄａは初期値ｄａ’＝１８に更新されるので、復号エラー発生確率が元に戻り、再び受信装置１２０ａは実用的に暗号化通信を行うことができるようになる。

【００９２】

実施の形態１では、送信装置１１０が暗号化通信時に用いる乱数多項式ｒを、期間が経過するにつれて、係数が１であるもの、及び係数が－１であるものの数を増加させるようにしている。これにより、受信装置１２０ａの有する秘密鍵多項式ｆａが暴露されたとしても、暴露された秘密鍵多項式ｆａを不正に用いる第三者の受信装置では、期間が経過するにつれて、復号エラーの発生確率が大きくなり、送信装置１１０が行う暗号化通信を正しく復号できなくなる。この結果、この暗号システム１は、従来技術と異なり、秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容が、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することができるようになる。

【００９３】

また、正規に秘密鍵多項式ｆａを有する受信装置１２０ａにおいても、期間が経過するにつれて、同じ秘密鍵多項式ｆａを使い続けると、徐々に復号エラーの発生確率が大きくなり、送信装置１１０が行う暗号化通信を正しく復号できなくなる。そして、受信装置１２０ａを扱うユーザに、同じ秘密鍵多項式ｆａを使い続けると、復号エラーの発生確率が大きくなっていき、鍵を更新しないと暗号化通信が実用にならなくなることを知らしめ、鍵の更新のために受信装置１２０の入力部１２６を介して、鍵再生成要求信号を入力することを促すことができる。この結果、この暗号システム１は、従来技術と異なり、受信装置又は受信装置を扱う人に、鍵の更新を促すことができるようになる。

【００９４】

さらに、この暗号システム１は、従来技術と異なり、第三者機関によるＣＲＬやＳＲＭを必要としない。

【００９５】

（実施の形態２）

本発明の実施の形態２における暗号システム２は、暗号システム１を基本にして構成した、映画や音楽などのデジタル著作物（以降、コンテンツと呼ぶ）の配信に適した暗号システムである。

【００９６】

平文多項式ｍをＮＴＲＵ暗号で暗号化して送信する代わりに、デジタルデータであるコンテンツＣＮＴｉ（１≦ｉ≦ｋ）を暗号鍵Ｋｉ（１≦ｉ≦ｋ）を用いて共通鍵暗号で暗号化し、その暗号鍵Ｋｉ（１≦ｉ≦ｋ）をＮＴＲＵ暗号で暗号化して、暗号化したコンテンツと暗号化した暗号鍵を送信する点が暗号システム１と異なる。また、鍵サーバを利用して鍵の更新を行う点が暗号システム１と異なる。以下に詳細を説明する。

【００９７】

実施の形態２における暗号システム２の全体構成を図１１に示す。この暗号システム２はコンテンツＣＮＴの配信を行うシステムであり、コンテンツサーバ２１０と、鍵サーバ２２０と、受信装置２３０とから構成され、コンテンツサーバ２１０と受信装置２３０はインターネット２４０を介して接続されており、コンテンツサーバ２１０と鍵サーバ２２０は専用回線２５０で接続されており、鍵サーバ２２０と受信装置２３０とは、電話回線２６０で接続されている。

【００９８】

コンテンツサーバ２１０は、コンテンツＣＮＴをユーザｊに提供する業者が有しており、鍵サーバ２２０は、コンテンツＣＮＴを利用するための復号鍵をユーザｊに提供する業者が有しており、受信装置２３０は、コンテンツＣＮＴを利用するユーザｊが有している。

【００９９】

以下に、これらの構成要素について詳細に説明を行う。

【０１００】

コンテンツサーバ２１０は、図１２に示すように、コンテンツ記憶部２１１、パラメータ記憶部２１２、タイマ部２１３、パラメータ制御部２１４、乱数生成部２１５、暗号鍵生成部２１６、暗号化部２１７、送信部２１８及び鍵更新部２１９から構成される。

【０１０１】

コンテンツ記憶部２１１は、外部より入力されたコンテンツＣＮＴを、例えば一定時間毎に区切ったＭＰＥＧ２データＣＮＴｉ（１≦ｉ≦ｋ）として格納している。

【０１０２】

パラメータ記憶部２１２は、図１３に示すように、ユーザｊ毎に、受信装置２３０の固有番号ＩＤｊ、公開鍵多項式ｈｊ及び乱数パラメータｄｊを、一組のデータＤＴｊ＝（ＩＤｊ，ｈｊ，ｄｊ）（１≦ｊ≦ｎ）として記憶している。ここで、乱数パラメータｄｊは、暗号化時に用いる乱数多項式ｒｉ（１≦ｉ≦ｋ）を生成するためのパラメータであり、乱数多項式ｒｉ（１≦ｉ≦ｋ）の係数のうち、係数が１であるものの数、及び係数が－１であるものの数である。なお、乱数パラメータｄｊの初期値は、ｄｊ＝１８とする。

【０１０３】

タイマ部２１３は、一日毎に時間信号を発生し、パラメータ制御部２１４に入力する。

【０１０４】

パラメータ制御部２１４は、タイマ部２１３から時間信号を受け取ったら、パラメータ記憶部２１２に記憶されたデータＤＴｊの乱数パラメータｄｊ（１≦ｊ≦ｎ）の値を１ずつ増加させる。

【０１０５】

乱数生成部２１５は、パラメータ記憶部２１２から送信装置２３０の乱数パラメータｄｊを読み出す。そして、読み出した乱数パラメータｄｊに基づき、ｄｊ個の係数が１であり、かつｄｊ個の係数が－１であり、かつその他の係数が０となる乱数多項式ｒｉ（１≦ｉ≦ｋ）をランダムに生成する。そして、生成した乱数多項式ｒｉ（１≦ｉ≦ｋ）を暗号化部２１７へ出力する。

【０１０６】

暗号鍵生成部２１６は、ランダムに暗号鍵Ｋｉ（１≦ｉ≦ｋ）を生成し、暗号化部２１７へ出力する。

【０１０７】

暗号化部２１７は、予めＮＴＲＵ暗号方式の暗号アルゴリズムＥと、例えばＤＥＳ暗号方式のような共通鍵暗号アルゴリズムＳｙｍを有している。

【０１０８】

共通鍵暗号では、暗号鍵Ｋを用いて、平文ｍに共通鍵暗号アルゴリズムＳｙｍを施して、暗号文ｃ＝Ｓｙｍ（ｍ，Ｋ）を生成し、暗号鍵Ｋを用いて、暗号文ｃに共通鍵暗号アルゴリズムＳｙｍを施して、復号文ｍ’＝Ｓｙｍ（ｃ，Ｋ）を生成する。ここで、暗号文生成時に用いた暗号鍵Ｋと復号文生成時に用いる暗号鍵Ｋが同一であれば、ｍ’＝ｍとなる。なお、共通鍵暗号及びＤＥＳ暗号方式については、非特許文献１に詳しく述べられているため、ここでの詳細な説明は省略する。

【０１０９】

暗号化部２１７は、暗号鍵生成部２１６から暗号鍵Ｋｉ（１≦ｉ≦ｋ）を受け取り、受け取った暗号鍵Ｋｉ（１≦ｉ≦ｋ）をＮＴＲＵ暗号で暗号化できるように暗号鍵多項式ＫＰｉ（１≦ｉ≦ｋ）に変換する。この変換は、暗号鍵Ｋｉをビット列としたとき、例えば、暗号鍵Ｋｉの下位ｂビット目の値をＸ＾ｂの係数として暗号鍵多項式ＫＰｉを構成することで実現できる。すなわち、Ｋｉ＝１００１０（ビット表現）の場合、ＫＰｉ＝Ｘ＾５＋Ｘ＾２となる。

【０１１０】

そして、暗号化部２１７は、パラメータ記憶部２１２から受信装置２３０の公開鍵多項式ｈｊを読み出し、乱数生成部２１５から乱数多項式ｒｉ（１≦ｉ≦ｋ）を受け取る。そして、暗号化部２１７は、乱数多項式ｒｉ（１≦ｉ≦ｋ）と公開鍵多項式ｈｊを用いて、変換した暗号鍵多項式ＫＰｉ（１≦ｉ≦ｋ）にＮＴＲＵ暗号方式の暗号アルゴリズムＥを施して、暗号化暗号鍵多項式ＥＫＰｉ＝Ｅ（ＫＰｉ，ｒｉ，ｈｊ）（１≦ｉ≦ｋ）を生成する。

【０１１１】

そして、暗号化部２１７は、コンテンツ記憶部２１１から、コンテンツＣＮＴｉ（１≦ｉ≦ｋ）を受け取り、前記暗号鍵Ｋｉ（１≦ｉ≦ｋ）を使用して、コンテンツＣＮＴｉ（１≦ｉ≦ｋ）に共通鍵暗号アルゴリズムＳｙｍを施して、暗号化コンテンツＥＣｉ＝Ｓｙｍ（ＣＮＴｉ，Ｋｉ）（１≦ｉ≦ｋ）を生成する。

【０１１２】

そして、暗号化部２１７は、暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を送信部２１８へ出力する。

【０１１３】

送信部２１８は、暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を、インターネット２４０を介して受信装置２３０へ送信する。

【０１１４】

鍵更新部２１９は、専用回線２５０を介して鍵サーバ２２０から、受信装置２３０の固有番号ＩＤｊと公開鍵多項式ｈｊ’（１≦ｊ≦ｎ）を受信することができる。もしも、受信装置２３０の固有番号ＩＤｊと公開鍵多項式ｈｊ’（１≦ｊ≦ｎ）を受信した場合、鍵更新部２１９は、パラメータ記憶部２１２に記憶されているデータＤＴｊ＝（ＩＤｊ，ｈｊ，ｄｊ）を、ＤＴｊ’＝（ＩＤｊ，ｈｊ’，ｄｊ’）に更新する。ここでｄｊ’は、乱数パラメータｄｊの初期値であり、ｄｊ’＝１８である。

【０１１５】

以上に述べたコンテンツサーバ２１０は、以下に述べる暗号化通信処理、乱数パラメータ更新処理及び公開鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

【０１１６】

以下に、コンテンツサーバ２１０の動作について、暗号化通信処理、乱数パラメータ更新処理、公開鍵更新処理に分けて説明を行う。

【０１１７】

最初に、コンテンツサーバ２１０の暗号化通信処理について、図１４に示すフローチャートを用いて説明する。

【０１１８】

まず、乱数生成部２１５は、パラメータ記憶部２１２から受信装置２３０の乱数パラメータｄｊを読み出し（ステップＳ２０１）、そして、読み出した乱数パラメータｄｊに基づき、ｄｊ個の係数が１であり、かつｄｊ個の係数が－１であり、かつその他の係数が０となる乱数多項式ｒｉ（１≦ｉ≦ｋ）をランダムに生成し、生成した乱数多項式ｒｉ（１≦ｉ≦ｋ）を暗号化部２１７へ出力する（ステップＳ２０２）。

【０１１９】

次に、暗号鍵生成部２１６は、ランダムに暗号鍵Ｋｉ（１≦ｉ≦ｋ）を生成し、生成した暗号鍵Ｋｉ（１≦ｉ≦ｋ）を暗号化部２１７へ出力する（ステップＳ２０３）。

【０１２０】

次に、暗号化部２１７は、暗号鍵生成部２１６から暗号鍵Ｋｉ（１≦ｉ≦ｋ）を受け取り、受け取った暗号鍵Ｋｉ（１≦ｉ≦ｋ）をＮＴＲＵ暗号で暗号化できるように暗号鍵多項式ＫＰｉ（１≦ｉ≦ｋ）に変換し（ステップＳ２０４）、そして、コンテンツ記憶部２１１からコンテンツＣＮＴｉ（１≦ｉ≦ｋ）を読み出し、パラメータ記憶部２１２から受信装置２３０の公開鍵多項式ｈｊを読み出し、乱数生成部２１５から乱数多項式ｒｉ（１≦ｉ≦ｋ）を受け取る（ステップＳ２０５）。そして、暗号化部２１７は、乱数多項式ｒｉ（１≦ｉ≦ｋ）と公開鍵多項式ｈｊを用いて、変換した暗号鍵多項式ＫＰｉ（１≦ｉ≦ｋ）にＮＴＲＵ暗号方式の暗号アルゴリズムＥを施して、暗号化暗号鍵多項式ＥＫＰｉ＝Ｅ（ＫＰｉ，ｒｉ，ｈｊ）（１≦ｉ≦ｋ）を生成する（ステップＳ２０６）。そして、暗号化部２１７は、コンテンツ記憶部２１１から、コンテンツＣＮＴｉ（１≦ｉ≦ｋ）を受け取り、前記暗号鍵Ｋｉ（１≦ｉ≦ｋ）を使用して、コンテンツＣＮＴｉ（１≦ｉ≦ｋ）に共通鍵暗号アルゴリズムＳｙｍを施して、暗号化コンテンツＥＣｉ＝Ｓｙｍ（ＣＮＴｉ，Ｋｉ）（１≦ｉ≦ｋ）を生成し（ステップＳ２０７）、そして、暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を送信部２１８へ出力する（ステップＳ２０８）。

【０１２１】

次に、送信部２１８は、受け取った暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）をインターネット２４０を介して受信装置２３０へ送信して処理を終了する（ステップＳ２０９）。

【０１２２】

次に、コンテンツサーバ２１０の乱数パラメータ更新処理について、図１５に示すフローチャートを用いて説明する。

【０１２３】

まず、パラメータ制御部２１４は、タイマ部２１３から時間信号を受け取ったら、ステップＳ２１２へ処理を移し、そうでなければ処理を終了する（ステップＳ２１２）。

【０１２４】

そして、パラメータ制御部２１４は、パラメータ記憶部２１２に記憶されている乱数パラメータｄｊ（１≦ｊ≦ｎ）を１ずつ増加させて、処理を終了する（ステップＳ２１２）。

【０１２５】

次に、コンテンツサーバ２１０の公開鍵更新処理について、図１６に示すフローチャートを用いて説明する。

【０１２６】

まず、鍵更新部２１９は、専用回線２５０を介して鍵サーバ２２０から、受信装置２３０の固有番号ＩＤｊと公開鍵多項式ｈｊ’（１≦ｊ≦ｎ）を受信したら、ステップＳ２２２へ処理を移し、そうでなければ処理を終了する（ステップＳ２２１）。

【０１２７】

そして、鍵更新部２１９は、パラメータ記憶部２１２に記憶されているデータＤＴｊ＝（ＩＤｊ，ｈｊ，ｄｊ）を、ＤＴｊ’＝（ＩＤｊ，ｈｊ’，ｄｊ’）に更新して処理を終了する。ここでｄｊ’は、乱数パラメータｄｊの初期値であり、ｄｊ’＝１８である（ステップＳ２２２）。

【０１２８】

鍵サーバ２２０は、図１７に示すように、ＩＤ受信部２２１、鍵再生成部２２

２、公開鍵送信部２２３及び秘密鍵送信部２２４から構成される。

【０１２９】

ＩＤ受信部２２１は、受信装置２３０から電話回線２６０を介して、受信装置２３０の固有番号ＩＤｊ（１≦ｊ≦ｎ）を受信すると、受信した固有番号ＩＤｊを鍵再生成部２２２に出力する。

【０１３０】

鍵再生成部２２２は、ＩＤ受信部２２１から固有番号ＩＤｊを受け取ると、ＮＴＲＵ暗号方式の秘密鍵多項式ｆｊ’と公開鍵多項式ｈｊ’を生成し、受け取った固有番号ＩＤｊと生成した公開鍵多項式ｈｊ’を公開鍵送信部２２３に出力し、生成した秘密鍵多項式ｆｊ’を秘密鍵送信部２２４に出力する。

【０１３１】

公開鍵送信部２２３は、鍵再生成部２２２から固有番号ＩＤｊと公開鍵多項式ｈｊ’を受け取ると、受け取った固有番号ＩＤｊと公開鍵多項式ｈｊ’を、専用回線２５０を介してコンテンツサーバ２１０へ送信する。

【０１３２】

秘密鍵送信部２２４は、鍵再生成部２２２から秘密鍵多項式ｆｊ’を受け取ると、受け取った秘密鍵多項式ｆｊ’を、電話回線２６０を介して受信装置２３０へ送信する。

【０１３３】

以上に述べた鍵サーバ２２０の動作について、図１８に示すフローチャートを用いて説明する。

【０１３４】

ＩＤ受信部２２１は、受信装置２３０から電話回線２６０を介して、受信装置２３０の固有番号ＩＤｊ（１≦ｊ≦ｎ）を受信したら、ステップＳ２３２へ処理を移し、そうでなければ処理を終了する（ステップＳ２３１）。ＩＤ受信部２２１は、受信した固有番号ＩＤｊを鍵再生成部２２２に出力する（ステップＳ２３２）。

【０１３５】

次に、鍵再生成部２２２は、ＩＤ受信部２２１から固有番号ＩＤを受け取り、

ＮＴＲＵ暗号方式の秘密鍵多項式ｆｊ’と公開鍵多項式ｈｊ’を生成し、受け取った固有番号ＩＤｊと生成した公開鍵多項式ｈｊ’を公開鍵送信部２２３に出力し、生成した秘密鍵多項式ｆｊ’を秘密鍵送信部２２４に出力する（ステップＳ２３３）。

【０１３６】

次に、公開鍵送信部２２３は、鍵再生成部２２２から固有番号ＩＤｊと公開鍵多項式ｈｊ’を受け取り、受け取った固有番号ＩＤｊと公開鍵多項式ｈｊ’を、専用回線２５０を介してコンテンツサーバ２１０へ送信する（ステップＳ２３４）。

【０１３７】

次に、秘密鍵送信部２２４は、鍵再生成部２２２から秘密鍵多項式ｆｊ’を受け取り、受け取った秘密鍵多項式ｆｊ’を、電話回線２６０を介して受信装置２３０へ送信する（ステップＳ２３５）。

【０１３８】

受信装置２３０は、図１９に示すように、受信部２３１、秘密鍵記憶部２３２、復号化部２３３、出力部２３４、鍵更新用送受信部２３５、及び入力部２３６から構成される。

【０１３９】

受信部２３１は、コンテンツサーバ２１０からインターネット２４０を介して、暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を受信し、受信した暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を復号化部２３３へ出力する。

【０１４０】

秘密鍵記憶部２３２は、受信装置３２０の秘密鍵多項式ｆｊを記憶している。

【０１４１】

復号化部２３３は、暗号化部２１７が有する暗号アルゴリズムＥの逆変換である、ＮＴＲＵ暗号方式の復号アルゴリズムＤと、暗号化部２１７が有する共通鍵暗号アルゴリズムＳｙｍを予め有している。

【０１４２】

復号化部２３３は、受信部２３１から暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を受け取り、秘密鍵記憶部２３２から受信装置２３０の秘密鍵多項式ｆｊを読み出す。そして、復号化部２３３は、秘密鍵多項式ｆｊを用いて、暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）に前記復号アルゴリズムＤを施して、復号暗号鍵多項式ＫＰｉ’＝Ｄ（ＥＫＰｉ，ｆｊ）（１≦ｉ≦ｋ）を生成する。

【０１４３】

そして、復号化部２３３は、コンテンツサーバ２１０の暗号化部２１７における変換の逆変換を用いて、復号暗号鍵多項式ＫＰｉ（１≦ｉ≦ｋ）を復号暗号鍵Ｋｉ（１≦ｉ≦ｋ）に変換する。

【０１４４】

そして、復号化部２３３は、復号暗号鍵Ｋｉ’（１≦ｉ≦ｋ）を使用して、暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）に共通鍵暗号アルゴリズムＳｙｍを施して、復号コンテンツＣＮＴｉ’＝Ｓｙｍ（ＥＣｉ，Ｋｉ’）（１≦ｉ≦ｋ）を生成し、復号コンテンツＣＮＴｉ’（１≦ｉ≦ｋ）を出力部２３４に出力する。

【０１４５】

出力部２３４は、例えばモニタやスピーカ等を備えており、入力された復号コンテンツＣＮＴｉ’（１≦ｉ≦ｋ）を外部に出力する。

【０１４６】

モニタは、復号コンテンツＣＮＴｉ’（１≦ｉ≦ｋ）のＭＰＥＧ２データから得られる映像を外部に出力し、スピーカ３３５は、復号コンテンツＣＮＴｉ’（１≦ｉ≦ｋ）のＭＰＥＧ２データから得られる音声を外部に出力する。

【０１４７】

鍵更新用送受信部２３５は、入力部２３６を介して鍵再生成要求信号を受け取った場合、受信装置２３０の固有番号ＩＤｊを、電話回線２６０を介して鍵サーバ２２０へ送信し、鍵サーバ２２０から電話回線２６０を介して、秘密鍵多項式ｆｊ’を受信して、秘密鍵記憶部２３２に記憶されている秘密鍵多項式ｆｊを受信した秘密鍵多項式ｆｊ’に更新する。

【０１４８】

受信装置２３０を扱うユーザｊは、受信装置２３０の公開鍵多項式ｈｊと秘密鍵多項式ｆｊの再生成を指示する鍵再生成要求信号を入力部３３５に入力することができる。この鍵再生成要求信号は、出力部２３４から出力された復号コンテンツＣＮＴｉ’（１≦ｉ≦ｋ）が正しく得られない等の理由で、ユーザが公開鍵多項式ｈｊと秘密鍵多項式ｆｊの再生成のために入力する信号である。

【０１４９】

入力部２３６は、外部から入力された鍵再生成要求信号を鍵更新用送受信部２３５に出力する。

【０１５０】

以上に述べた受信装置２３０は、以下に述べる復号化処理及び鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

【０１５１】

以下に、受信装置２３０の動作について、復号化処理、鍵更新処理に分けて説明を行う。

【０１５２】

最初に、受信装置２３０の復号化処理について、図２０に示すフローチャートを用いて説明する。

【０１５３】

まず、受信部２３１は、コンテンツサーバ２１０からインターネット２４０を介して、暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を受信し、受信した暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を復号化部２３３へ出力する（ステップＳ２５１）。

【０１５４】

次に、復号化部２３３は、受信部２３１から暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を受け取り、秘密鍵記憶部２３２から受信装置２３０の秘密鍵多項式ｆｊを読み出し（ステップＳ２５２）、そして、秘密鍵多項式ｆｊを用いて、暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）に復号アルゴリズムＤを施して、復号暗号鍵多項式ＫＰｉ’＝Ｄ（ＥＫＰｉ

，ｆｊ）（１≦ｉ≦ｋ）を生成する（ステップＳ２５３）。

【０１５５】

次に、復号化部２３３は、コンテンツサーバ２１０の暗号化部２１７における変換の逆変換を用いて、復号暗号鍵多項式ＫＰｉ（１≦ｉ≦ｋ）を復号暗号鍵Ｋｉ（１≦ｉ≦ｋ）に変換する（ステップＳ２５４）。

【０１５６】

次に、復号化部２３３は、復号暗号鍵Ｋｉ’（１≦ｉ≦ｋ）を使用して、暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）に共通鍵暗号アルゴリズムＳｙｍを施して、復号コンテンツＣＮＴｉ’＝Ｓｙｍ（ＥＣｉ，Ｋｉ’）（１≦ｉ≦ｋ）を生成し、復号コンテンツＣＮＴｉ’（１≦ｉ≦ｋ）を出力部２３４に出力する（ステップＳ２５５）。

【０１５７】

次に、出力部２３４は、それぞれ、復号コンテンツＣＮＴｉ’（１≦ｉ≦ｋ）のＭＰＥＧ２データから得られる映像及び音声を外部に出力して処理を終了する（ステップＳ２５６）。

【０１５８】

次に、受信装置２３０の鍵更新処理について、図２１に示すフローチャートを用いて説明する。

【０１５９】

まず、鍵更新用送受信部２３５は、もしも、入力部２３６を介して鍵再生成要求信号を受け取ったら、ステップＳ２６２へ処理を移し、そうでなければ処理を終了する（ステップＳ２６１）。

【０１６０】

次に、鍵更新用送受信部２３５は、受信装置２３０の固有番号ＩＤｊを、電話回線２６０を介して鍵サーバ２２０へ送信し（ステップＳ２６２）、鍵サーバ２２０から電話回線２６０を介して、秘密鍵多項式ｆｊ’を受信して、秘密鍵記憶部２３２に記憶されている秘密鍵多項式ｆｊを受信した秘密鍵多項式ｆｊ’に更新して処理を終了する（ステップＳ２６３）。

【０１６１】

以下に、実施の形態２における暗号システム２全体の動作について暗号システム１との差異点を中心に説明する。

【０１６２】

まず、コンテンツサーバ２１０は、受信装置２３０の固有番号ＩＤｊ、公開鍵多項式ｈｊ及び乱数パラメータｄｊを、データＤＴｊ＝（ＩＤｊ，ｈｊ，ｄｊ）としてパラメータ記憶部２１２に記憶している。乱数パラメータｄｊの初期値は、ｄｊ＝１８である。

【０１６３】

そして、コンテンツサーバ２１０は暗号化通信処理に従って、コンテンツＣＮＴｉ（１≦ｉ≦ｋ）を暗号鍵Ｋｉ（１≦ｉ≦ｋ）を用いて共通鍵暗号で暗号化して暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を生成し、その暗号鍵Ｋｉ（１≦ｉ≦ｋ）から変換した暗号鍵多項式ＫＰｉ（１≦ｉ≦ｋ）をＮＴＲＵ暗号で暗号化して暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）を生成し、暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）と共にインターネット２４０を介して受信装置２３０に送信する。一方、受信装置２３０は復号化処理に従って、暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）と暗号化暗号鍵ＥＫｉ（１≦ｉ≦ｋ）をインターネット２４０を介して送信装置２１０から受信し、受信した暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）を復号して復号暗号鍵多項式ＫＰｉ’（１≦ｉ≦ｋ）を生成し、これを変換した復号暗号鍵Ｋｉ（１≦ｉ≦ｋ）を用いて、暗号化コンテンツＥＣｉ（１≦ｉ≦ｋ）を復号して復号コンテンツＣＮＴｉ’（１≦ｉ≦ｋ）を出力する。

【０１６４】

なお、コンテンツサーバ２１０では、乱数パラメータ更新処理に従って、タイマ部２１３が一日毎に発生する時間信号に応じて、パラメータ制御部２１４は、パラメータ記憶部２１２に記憶された全ての乱数パラメータｄｊ（１≦ｊ≦ｎ）の値を１ずつ増加させる。すなわち、パラメータ記憶部２１２に記憶された全ての乱数パラメータｄｊ（１≦ｉ≦ｎ）の値は一日毎に増加する。

【０１６５】

従って、このコンテンツサーバ２１０の暗号化通信処理が継続して行われると

、暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）を生成される際に用いられる乱数多項式ｒｉ（１≦ｉ≦ｋ）は、係数が１であるもの、及び係数が－１であるものの数が一日毎に増加する。

【０１６６】

今、図１０は、乱数パラメータｄの値に対し、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつその他の係数が０となる乱数多項式ｒを用いた場合の、ＮＴＲＵ暗号方式の復号エラー発生確率の測定結果である。この測定結果によれば、乱数パラメータｄｊの初期値ｄｊ＝１８においては、コンテンツサーバ２１０が生成する暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）は、ほとんど復号エラーは発生しない（受信装置２３０は受信した暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）から暗号鍵Ｋｉと等しい復号暗号鍵Ｋｉ’を得ることができて正しくコンテンツＣＮＴｉが復号できる）。一方で、期間が経過すれば、乱数パラメータｄｊが一日毎に徐々に大きくなるので、コンテンツサーバ２１０が生成する暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）は、徐々に復号エラー発生確率が大きくなる（受信装置２３０は受信した暗号化暗号鍵多項式ＥＫＰｉ（１≦ｉ≦ｋ）から暗号鍵Ｋｉと等しい復号暗号鍵Ｋｉ’を得ることが徐々にできなくなり、コンテンツＣＮＴｉを徐々に正しく復号できなくなる）。

【０１６７】

そして、もしも受信装置２３０がコンテンツＣＮＴｉ（１≦ｉ≦ｋ）を正しく復号できる確率が下がり、実用的な暗号化通信を行うことができなくなった場合、受信装置２３０を扱うユーザｊは、鍵更新処理を行うことにより、受信装置２３０の公開鍵多項式ｈｊと秘密鍵多項式ｆｊの再生成を指示する鍵再生成要求信号を入力部２３６に入力することができる。すると、鍵サーバ２２０により、コンテンツサーバ２１０のパラメータ記憶部２１２の乱数パラメータｄｊは初期値ｄｊ’＝１８に更新されるので、復号エラー発生確率が元に戻り、再び受信装置２３０は実用的に暗号化通信を行うことができるようになる。

【０１６８】

実施の形態２では、デジタルデータであるコンテンツＣＮＴを一定時間毎に分割し、ＣＮＴｉ（１≦ｉ≦ｋ）を受信装置２３０へ配信している。一般に、ＭＰ

ＥＧ２のようなデジタルデータの場合、復号エラーが発生して正しくＣＮＴｉが得られないと、動画像や音声にノイズが発生する。従って、期間が経過すると、復号エラーの発生確率が増加し、徐々に動画像や音声にノイズが増えることになる。これにより、コンテンツを提供する業者が、例えば１ヵ月間は実用上問題ないノイズ発生レベルでコンテンツをユーザに視聴させ、１ヵ月を過ぎると復号エラー発生確率が増加してノイズ発生レベルが大きくなり、鍵更新を行わない限りユーザがコンテンツを実用的に視聴できないようにさせることができる。すなわち、期間限定のコンテンツ配信に適する。

【０１６９】

また、一般に、ＭＰＥＧ２のようにサイズが大きいＣＮＴｉ（１≦ｉ≦ｋ）の場合、各ＣＮＴｉを全てＮＴＲＵ暗号で暗号化しようとすると、ＮＴＲＵ暗号の入力ビット長に合わせてＣＮＴｉを分割し、複数回ＮＴＲＵ暗号の暗号処理を行わなければならない。しかし、この場合、暗号鍵ＫｉをＮＴＲＵ暗号で暗号化し、サイズの大きいコンテンツＣＮＴｉは公開鍵暗号に比べて速度の速い共通鍵暗号で暗号化するので、高速処理が可能であり、コンテンツ配信に適する。

【０１７０】

また、鍵の更新時に、鍵サーバ２２０を利用するので、鍵サーバ２２０でユーザｊの鍵更新の回数を把握することができ、この回数によりコンテンツを提供する業者がユーザｊにコンテンツ配信の課金を行うこともできる。

【０１７１】

なお、実施の形態１で得られる効果も同様に得られる。

【０１７２】

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

【０１７３】

用いるＮＴＲＵ暗号のパラメータはＮ＝１６７に限定されず、他のパラメータでもよい。

【０１７４】

パラメータ制御部１１４、２１４では、一日毎に乱数パラメータを１ずつ増加させる以外に、期間が経過するにつれて徐々に増加させれば、任意の期間毎に乱数パラメータを増加させてもよいし、またパラメータの増加分を任意にしてもよい。

【０１７５】

さらに、パラメータ制御部１１４、２１４は、期間の経過に応じてではなく、乱数パラメータが読み出される毎に乱数パラメータを増加させてもよいし、乱数パラメータが読み出される回数に応じて乱数パラメータを増加させてもよい。これにより、暗号化回数が多くなるにつれ、徐々に復号エラー発生確率が大きくなるようにすることができるので、暴露された秘密鍵を有する第三者の受信装置に復号され続けることを防止でき、また受信装置又は受信装置を扱う人に鍵の更新を促すことができる。また、これにより、期間限定のコンテンツ配信以外にも、回数限定のコンテンツ配信にも利用できるようになる。

【０１７６】

鍵再生成要求信号は入力部１２６、２３６を介して外部から入力される代わりに、受信装置１２０、２３０、が何らかの方法で復号エラーを検知して、自動的に鍵再生要求信号が入力されるようにしてもよい。

【０１７７】

これは、例えば、実施の形態２における復号化部２３３が、さらに、復号コンテンツＣＮＴｉ’がＭＰＥＧ２のフォーマットに従っているかどうかを判別して復号エラーを検知し、復号エラー発生の度合が大きくなったら鍵再生成要求信号を入力部２３６に入力することで実現できる。また、例えば、平文多項式ｍや暗号鍵多項式ＫＰｉ（１≦ｉ≦ｋ）の高次の１０次元分の係数を１とする等、そのフォーマットを定めておき、復号化部１２３、２２３が、さらに、復号文多項式ｍ’や復号暗号鍵多項式ＫＰｉ’がそのフォーマットに従うかどうかを判別して復号エラーを検知し、復号エラー発生の度合が大きくなったら鍵再生成要求信号を入力部１２６、２３６に入力することでも実現できる。

【０１７８】

実施の形態２において、インターネット２４０、専用回線２５０、電話回線２

６０は、衛生通信網等の他の通信路を用いてもよいし、また同じ通信路を用いてもよい。なお、鍵サーバ２２０と受信装置２３０との間の通信路では、秘密鍵ｆｊの送信が行われるので、安全性を高めるために暗号化通信を行ってもよい。

【０１７９】

実施の形態２において、共通鍵暗号アルゴリズムＳｙｍとして、ＡＥＳ暗号等の他の共通鍵暗号方式を用いてもよい。

【０１８０】

実施の形態２において、コンテンツＣＮＴｉ（１≦ｉ≦ｋ）は、ＭＰＥＧ２データに限らず、Ｗｉｎｄｏｗｓ（Ｒ）ＭｅｄｉａＰｌａｙｅｒやＲｅａｌＰｌａｙｅｒで再生可能なデジタルデータでもよいし、そのデータの形式は限られない。

【０１８１】

実施の形態２において、コンテンツサーバ２１０と鍵サーバ３２０は同一システム内にあってもよい。

【０１８２】

本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【０１８３】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、半導体メモリ、ハードディスクドライブ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ，ＤＶＤ－ＲＡＭ等、に記録したものとしてもよい。

【０１８４】

上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０１８５】

【発明の効果】

以上に説明したように、本発明は、従来システムにおける問題点を鑑みて行われたもので、暗号システムにおいて、暗号化通信にＮＴＲＵ暗号方式を用い、送

信装置で乱数パラメータを期間が経過するにつれ増加させるようにしたので、期間が経過するにつれて、受信装置で暗号化通信を正しく復号できなくなるようにすることが可能となった。

【０１８６】

これにより、送信装置が暗号化通信を行うに際して、暴露された秘密鍵を不正に用いる第三者の受信装置は、期間が経過すると暗号化通信が復号できなくなる暗号化システム又は送信装置を提供でき、これにより秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容が、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することが可能となった。

【０１８７】

また、送信装置が暗号化通信を行うに際して、正規の受信者の受信装置は、復号を行うに従い、復号に失敗する確率が徐々に増大する暗号システム、送信装置又は受信装置を提供し、これにより受信装置又は受信装置を扱う人に、鍵の更新を促すようにすることが可能となった。

【０１８８】

さらに、送信装置が暗号化通信を行うに際して、第三者機関によるＣＲＬやＳＲＭを必要としない暗号システム、送信装置又は受信装置を提供することが可能となった。

【０１８９】

以上により、従来技術では達成できなかった暗号システムを提供することができ、その価値は大きい。

【図面の簡単な説明】

【図１】

本発明の実施の形態１における暗号システム１の構成を示す図

【図２】

本発明の実施の形態１における送信装置１１０の構成を示す図

【図３】

本発明の実施の形態１におけるパラメータ記憶部１１２の構成を示す図

【図４】

本発明の実施の形態１における送信装置１１０の暗号化通信処理の流れを示すフローチャート

【図５】

本発明の実施の形態１における送信装置１１０の乱数パラメータ更新処理の流れを示すフローチャート

【図６】

本発明の実施の形態１における送信装置１１０の公開鍵更新処理の流れを示すフローチャート

【図７】

本発明の実施の形態１における受信装置１２０ａの構成を示す図

【図８】

本発明の実施の形態１における受信装置１２０ａの復号化処理の流れを示すフローチャート

【図９】

本発明の実施の形態１における受信装置１２０ａの鍵更新処理の流れを示すフローチャート

【図１０】

ＮＴＲＵ暗号方式の復号エラー発生確率の測定結果を示す図

【図１１】

本発明の実施の形態２における暗号システム２の構成を示す図

【図１２】

本発明の実施の形態２におけるコンテンツサーバ２１０の構成を示す図

【図１３】

本発明の実施の形態２におけるパラメータ記憶部２１２の構成を示す図

【図１４】

本発明の実施の形態２におけるコンテンツサーバ２１０の暗号化通信処理の流れを示すフローチャート

【図１５】

本発明の実施の形態２におけるコンテンツサーバ２１０の乱数パラメータ更新

処理の流れを示すフローチャート

【図１６】

本発明の実施の形態２におけるコンテンツサーバ２１０の公開鍵更新処理の流れを示すフローチャート

【図１７】

本発明の実施の形態２における鍵サーバ２２０の構成を示す図

【図１８】

本発明の実施の形態２における鍵サーバ２２０の処理の流れを示すフローチャート

【図１９】

本発明の実施の形態２における受信装置２３０の構成を示す図

【図２０】

本発明の実施の形態２における受信装置２３０の復号化処理の流れを示すフローチャート

【図２１】

本発明の実施の形態２における受信装置２３０の鍵更新処理の流れを示すフローチャート

【符号の説明】

１，２　暗号システム

１１０　送信装置

１１１　平文入力部

１１２，２１２　パラメータ記憶部

１１３，２１３　タイマ部

１１４，２１４　パラメータ制御部

１１５，２１５　乱数生成部

１１６，２１７　暗号化部

１１７，２１８　送信部

１１８，２１９　鍵更新部

１２０ａ，１２０ｂ，１２０ｃ，２３０　受信装置

１２１，２３１　受信部

１２２，２３２　秘密鍵記憶部

１２３，２３３　復号化部

１２４　復号文出力部

１２５，２２２　鍵再生成部

１２６，２３６　入力部

１３０　通信路

２１０　コンテンツサーバ

２１１　コンテンツ記憶部

２１６　暗号鍵生成部

２２０　鍵サーバ

２２１　ＩＤ受信部

２２３　公開鍵送信部

２２４　秘密鍵送信部

２３４　出力部

２３５　鍵更新用送受信部

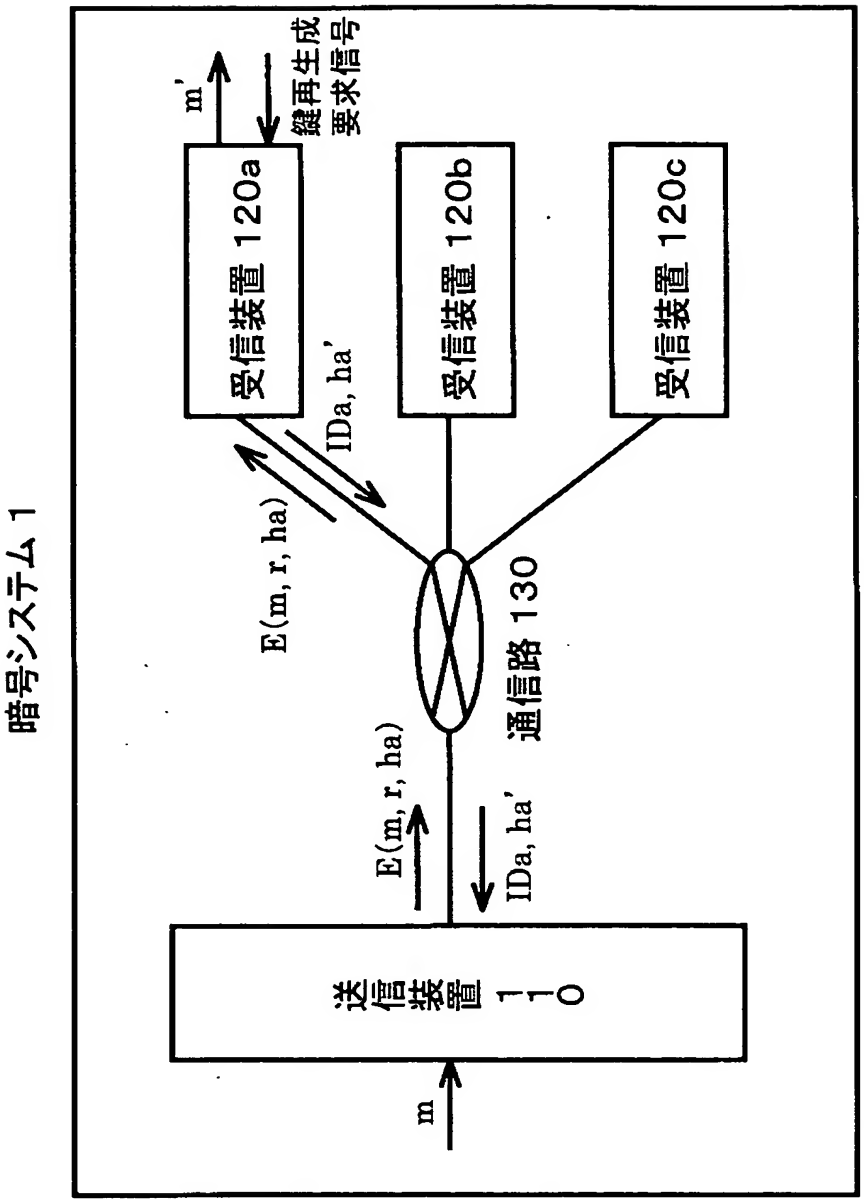
２４０　インターネット

２５０　専用回線

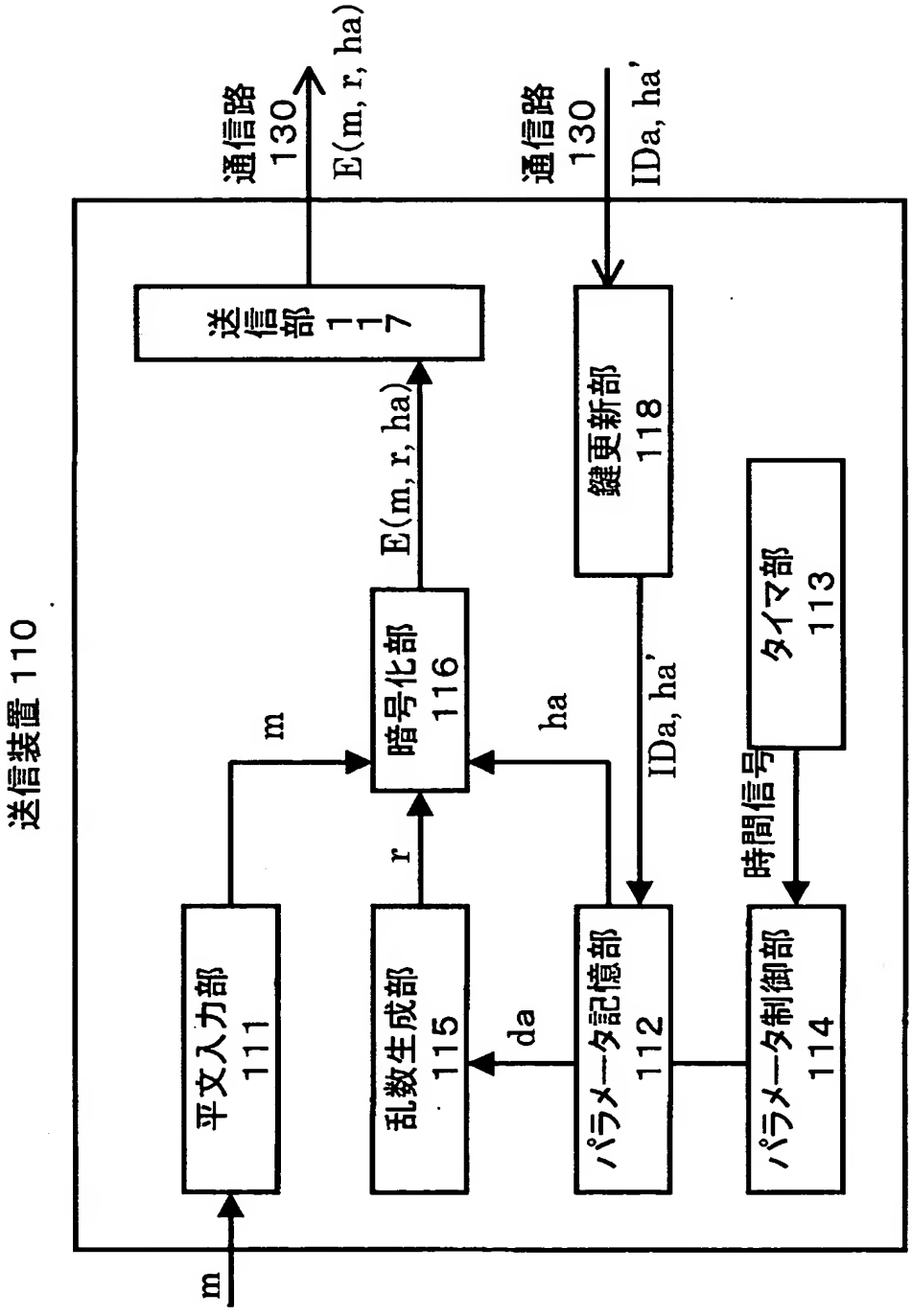
２６０　電話回線

【書類名】　　図面

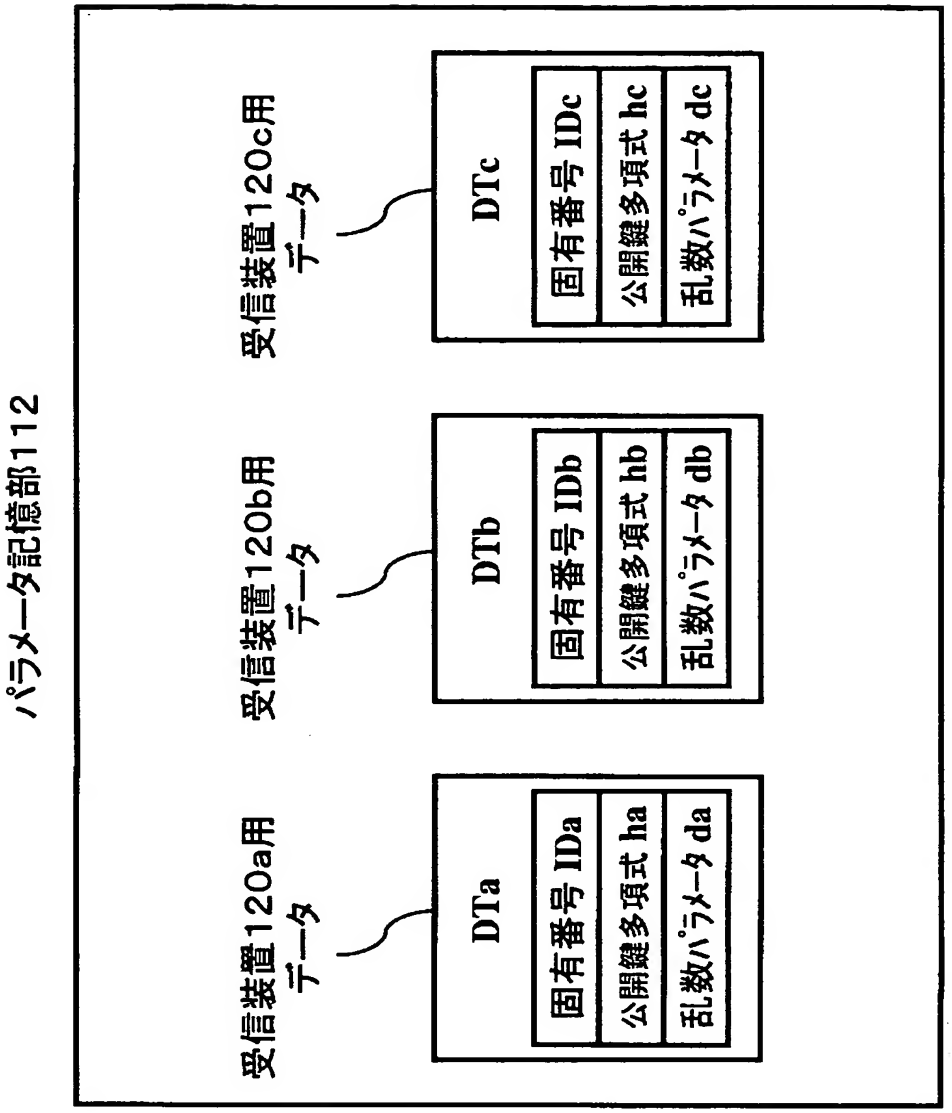
【図１】


暗号システム１
m'
鍵再生成要求信号
受信装置 120a
受信装置 120b
受信装置 120c
IDa, ha'
E(m, r, ha)
通信路 130
E(m, r, ha)
IDa, ha'
送信装置 110
m

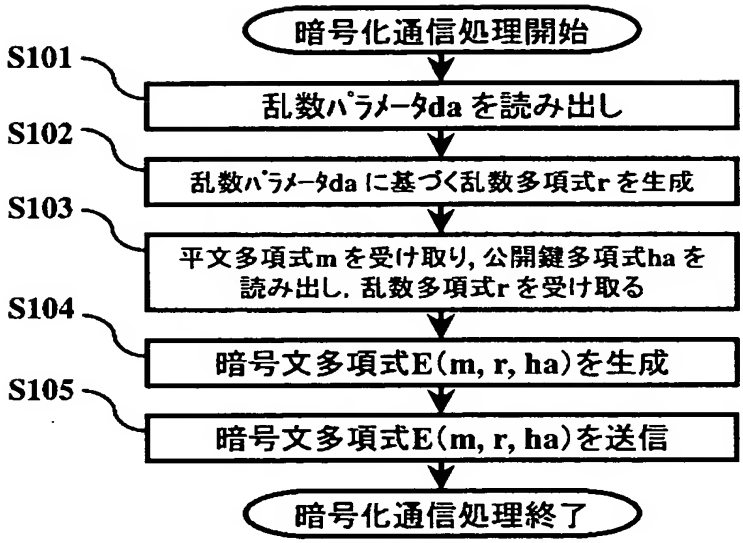
【図２】


送信装置 110
通信路 130
E(m, r, ha)
通信路 130
IDa, ha'
送信部 117
鍵更新部 118
E(m, r, ha)
暗号化部 116
タイマ部 113
m
ha
IDa, ha'
r
時間信号
平文入力部 111
乱数生成部 115
da
パラメータ記憶部 112
パラメータ制御部 114
m

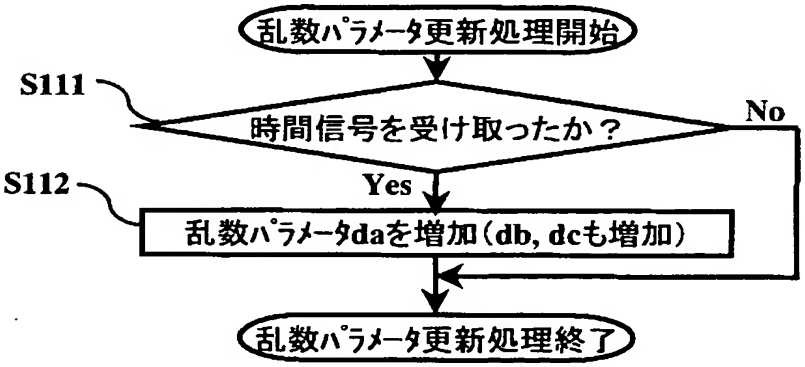
【図３】


パラメータ記憶部112
受信装置120a用データ
DTa
固有番号 IDa
公開鍵多項式 ha
乱数パラメータ da
受信装置120b用データ
DTb
固有番号 IDb
公開鍵多項式 hb
乱数パラメータ db
受信装置120c用データ
DTc
固有番号 IDc
公開鍵多項式 hc
乱数パラメータ dc

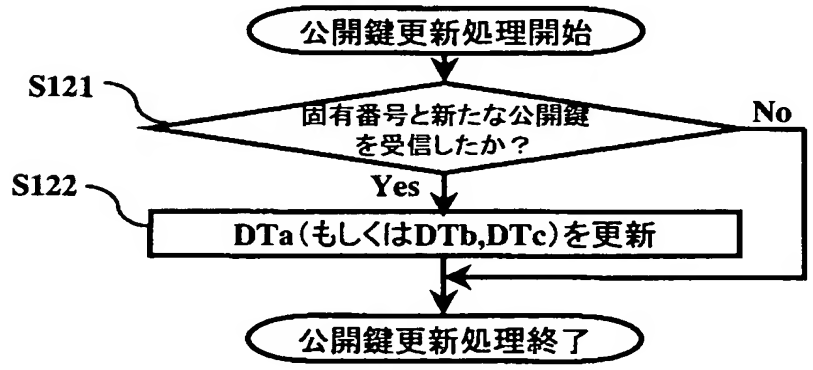
【図４】


暗号化通信処理開始
S101
乱数パラメータda を読み出し
S102
乱数パラメータda に基づく乱数多項式r を生成
S103
平文多項式m を受け取り, 公開鍵多項式ha を
読み出し. 乱数多項式r を受け取る
S104
暗号文多項式E(m, r, ha)を生成
S105
暗号文多項式E(m, r, ha)を送信
暗号化通信処理終了

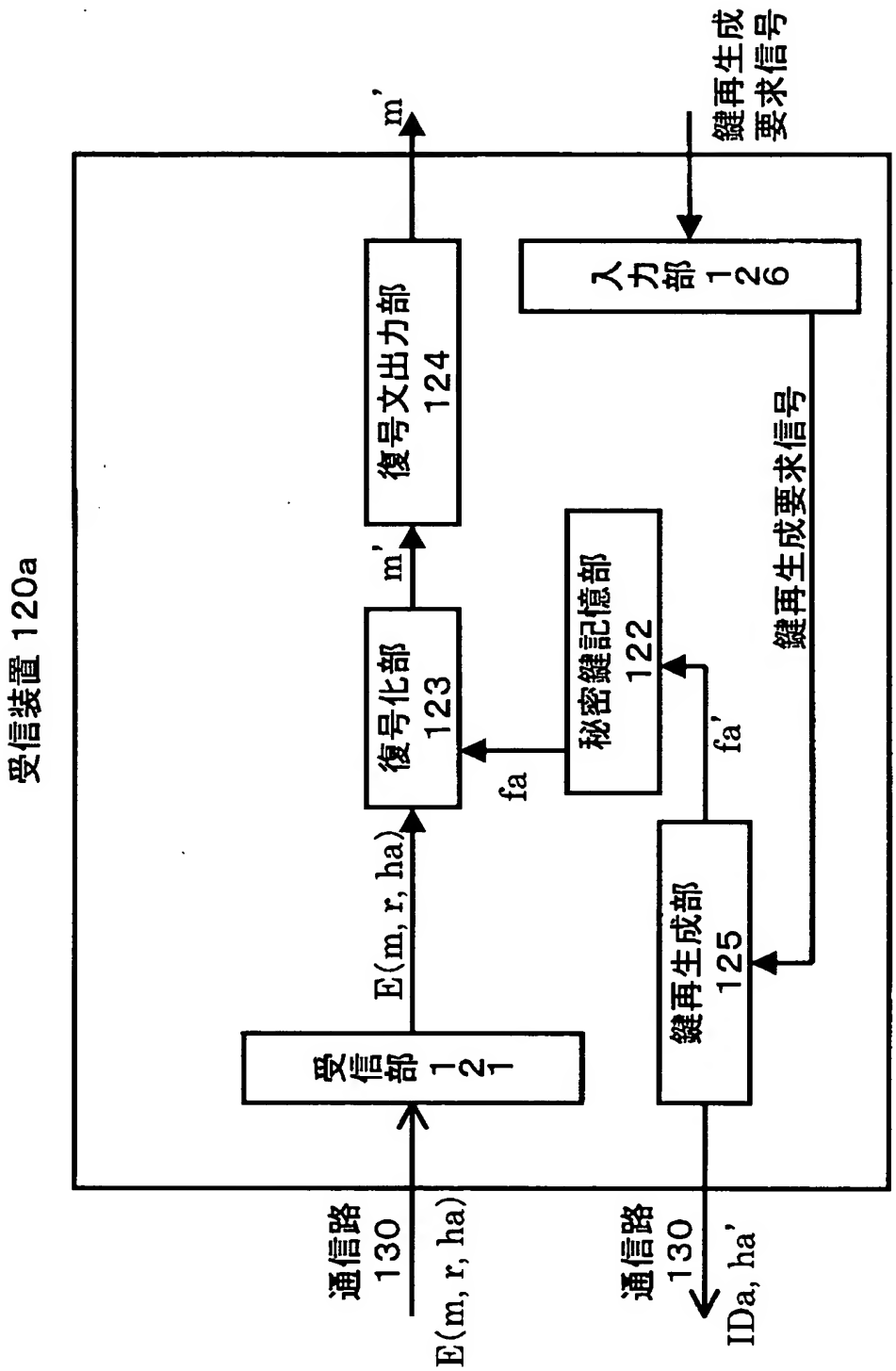
【図５】


乱数パラメータ更新処理開始
S111
時間信号を受け取ったか？
No
Yes
S112
乱数パラメータdaを増加(db, dcも増加)
乱数パラメータ更新処理終了

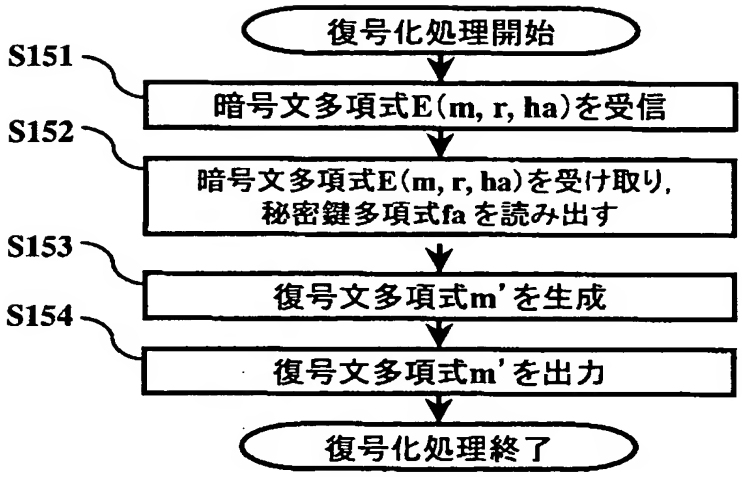
【図６】


公開鍵更新処理開始
S121
固有番号と新たな公開鍵
を受信したか？
No
Yes
S122
DTa(もしくはDTb,DTc)を更新
公開鍵更新処理終了

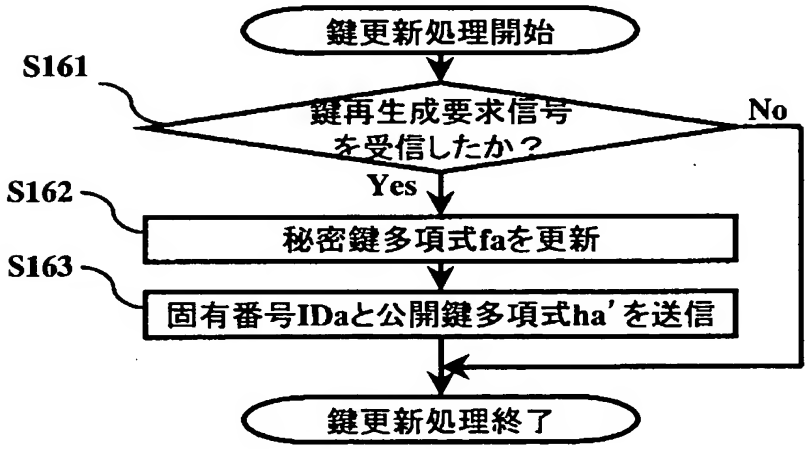
【図７】


受信装置 120a
通信路 130
E(m, r, ha)
受信部 121
E(m, r, ha)
復号化部 123
fa
秘密鍵記憶部 122
m'
復号文出力部 124
m'
通信路 130
IDa, ha'
鍵再生成部 125
fa'
鍵再生成要求信号
入力部 126
鍵再生成要求信号

【図８】


復号化処理開始
S151
暗号文多項式E(m, r, ha)を受信
S152
暗号文多項式E(m, r, ha)を受け取り,
秘密鍵多項式fa を読み出す
S153
復号文多項式m'を生成
S154
復号文多項式m'を出力
復号化処理終了

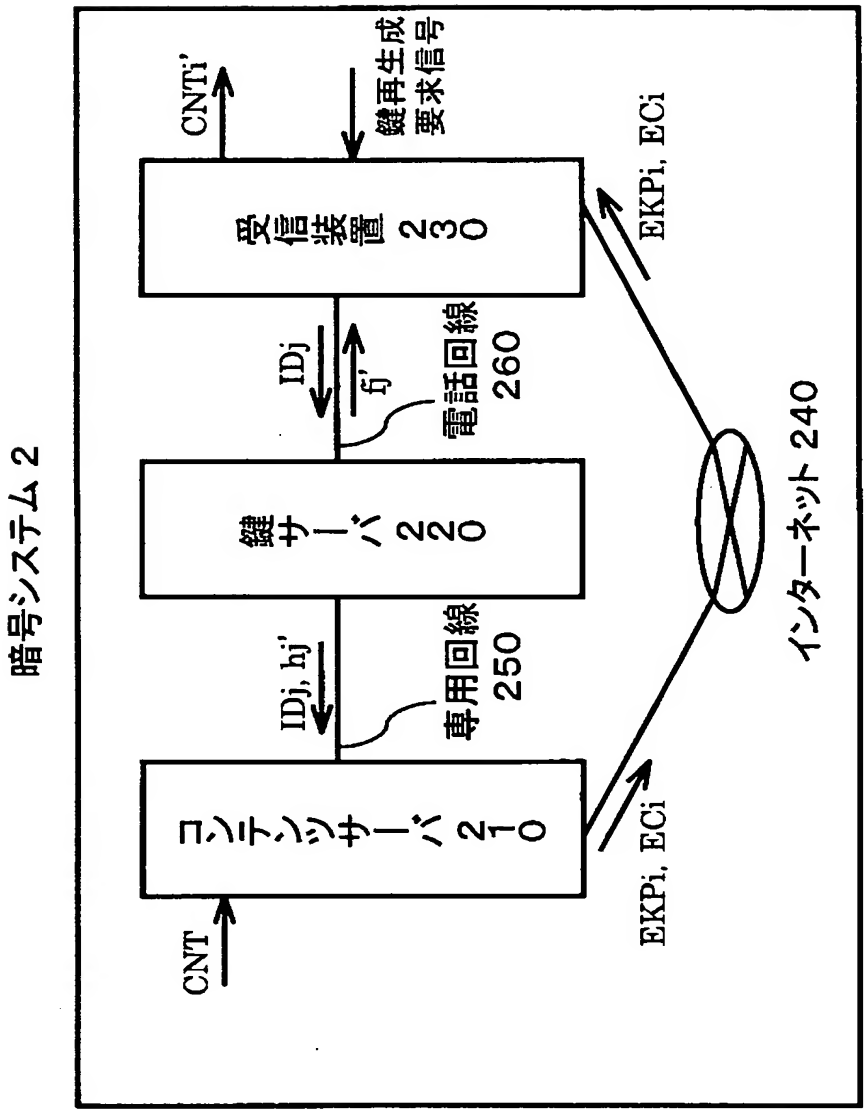
【図９】


鍵更新処理開始
S161
鍵再生成要求信号
を受信したか？
No
Yes
S162
秘密鍵多項式faを更新
S163
固有番号IDaと公開鍵多項式ha'を送信
鍵更新処理終了

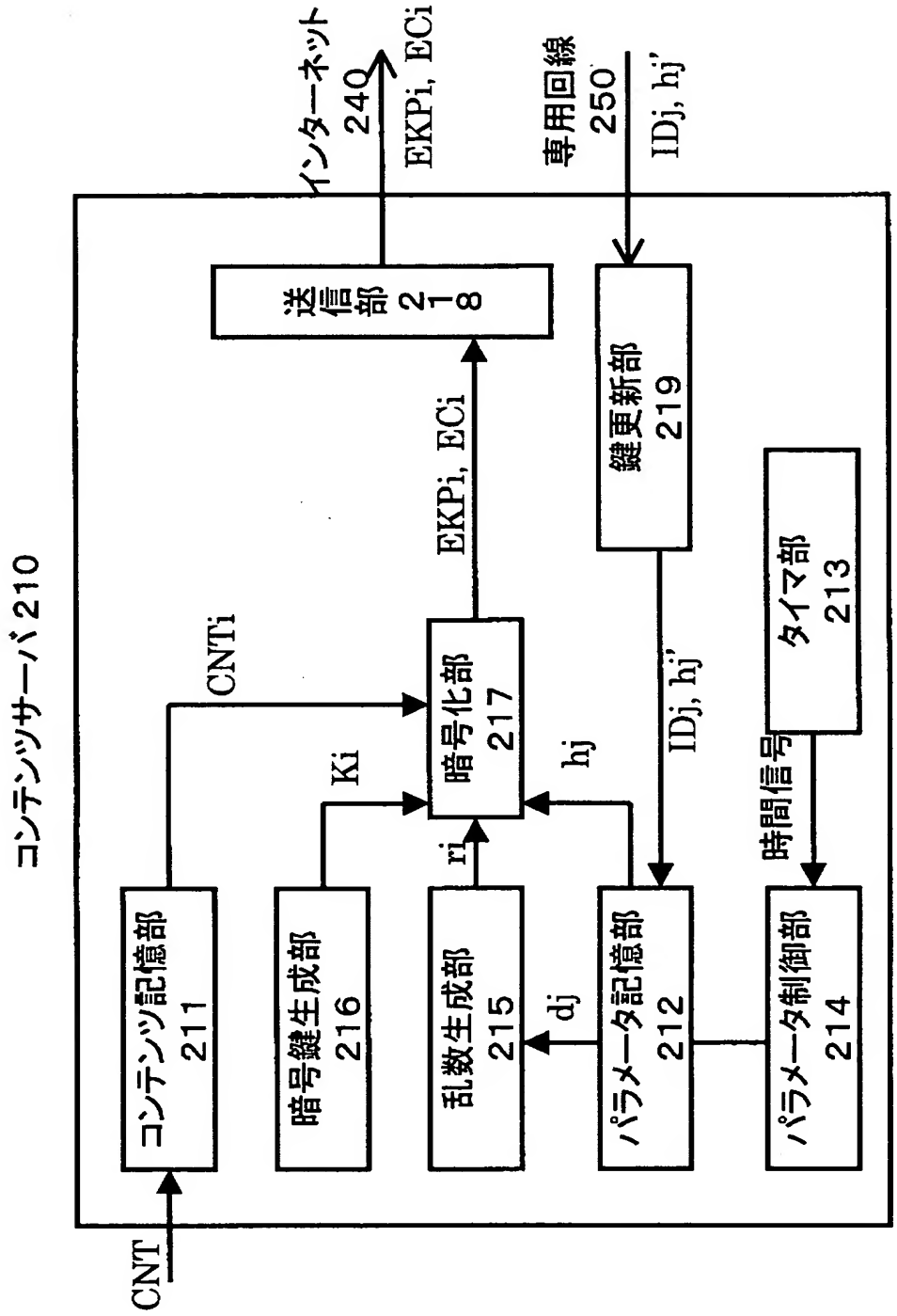
【図１０】

乱数パラメータｄ	18	28	38	48	58	68	78
復号エラー発生率(%)	0.0007	0.09	2.6	2.3	7.1	13.7	24.8

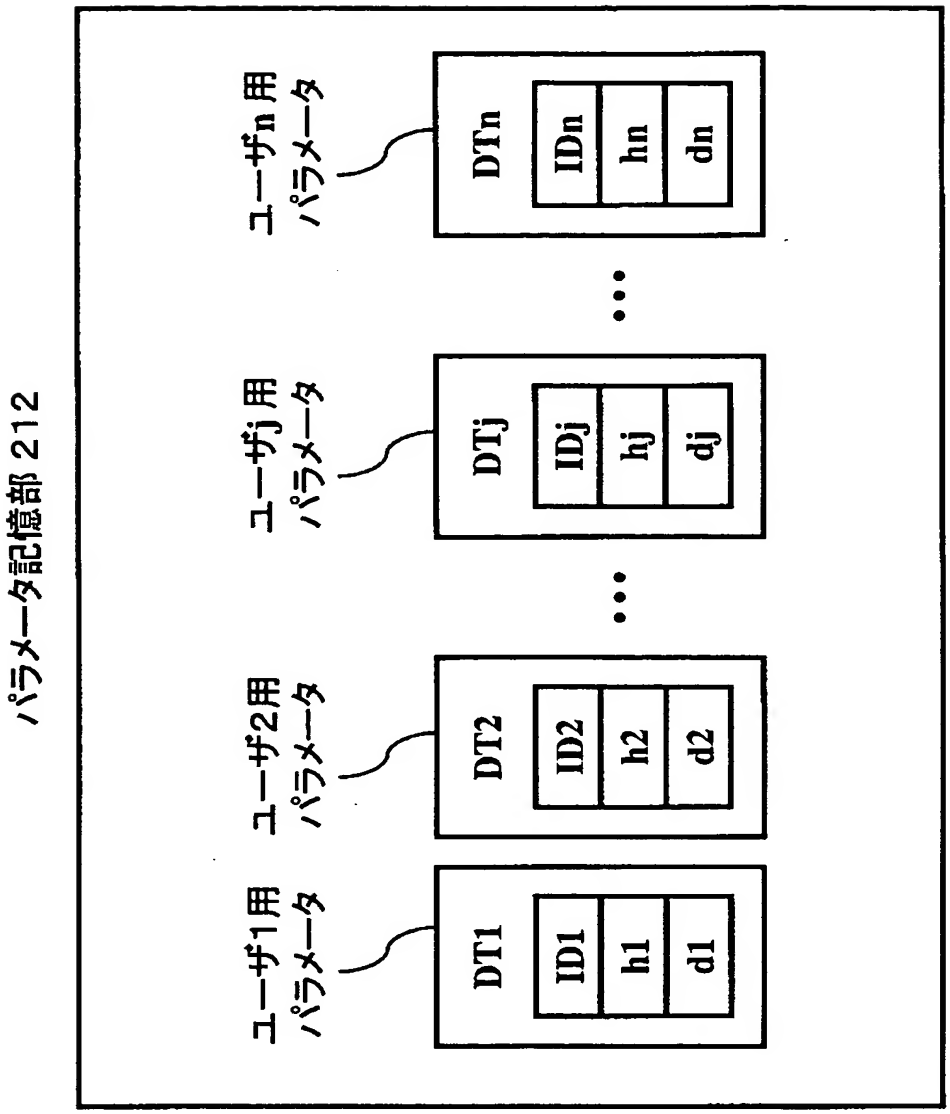
【図１１】


暗号システム２
コンテンツサーバ２１０
鍵サーバ２２０
受信装置２３０
専用回線２５０
電話回線２６０
インターネット２４０
CNT
CNTi'
鍵再生成要求信号
IDj, hj'
IDj
fj'
EKPi, ECi
EKPi, ECi

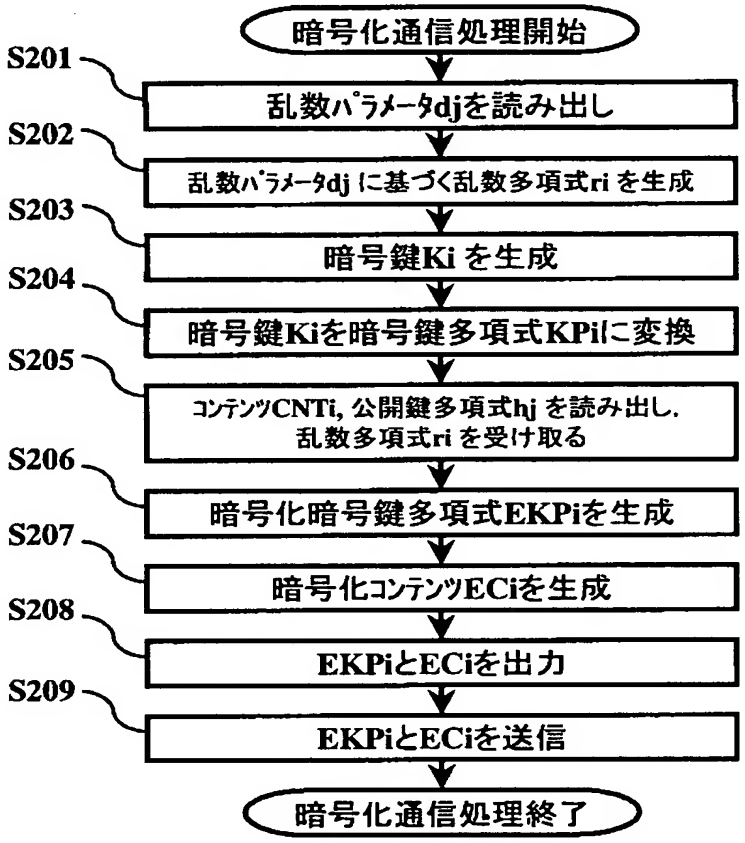
【図１２】


インターネット
240
EKPi, ECi
専用回線
250
IDj, hj'
コンテンツサーバ210
送信部 218
鍵更新部 219
タイマ部 213
EKPi, ECi
CNTi
暗号化部 217
Ki
hj
IDj, hj'
時間信号
ri
コンテンツ記憶部 211
暗号鍵生成部 216
乱数生成部 215
パラメータ記憶部 212
パラメータ制御部 214
dj
CNT

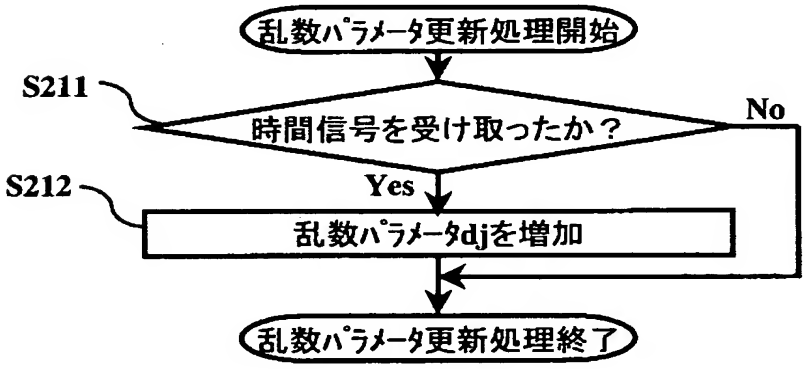
【図１３】


パラメータ記憶部 212
ユーザ1用 パラメータ
DT1
ID1
h1
d1
ユーザ2用 パラメータ
DT2
ID2
h2
d2
ユーザj用 パラメータ
DTj
IDj
hj
dj
ユーザn用 パラメータ
DTn
IDn
hn
dn

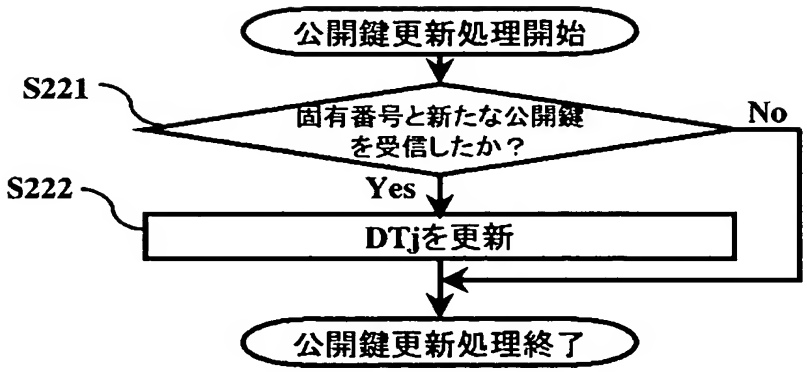
【図１４】


暗号化通信処理開始
S201
乱数パラメータdjを読み出し
S202
乱数パラメータdj に基づく乱数多項式ri を生成
S203
暗号鍵Ki を生成
S204
暗号鍵Kiを暗号鍵多項式KPiに変換
S205
コンテンツCNTi, 公開鍵多項式hj を読み出し.
乱数多項式ri を受け取る
S206
暗号化暗号鍵多項式EKPiを生成
S207
暗号化コンテンツECiを生成
S208
EKPiとECiを出力
S209
EKPiとECiを送信
暗号化通信処理終了

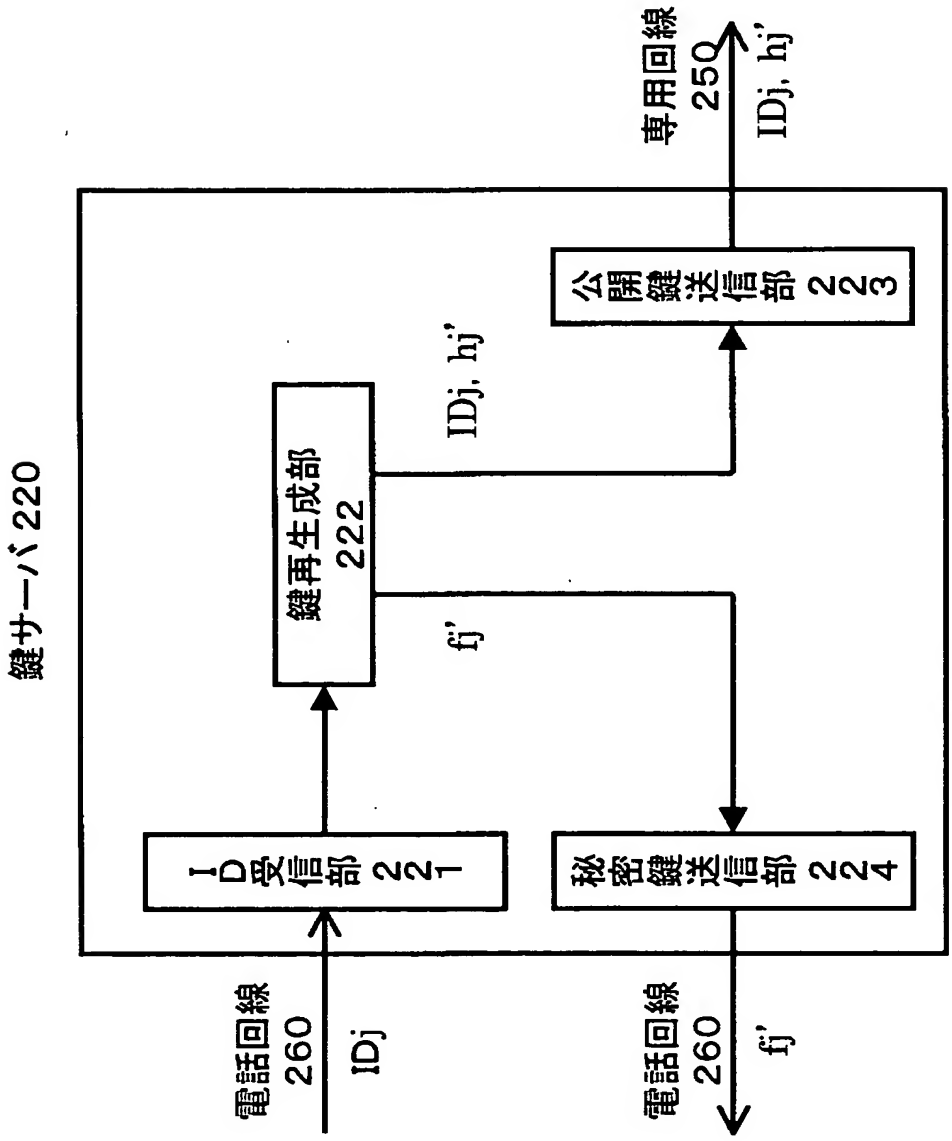
【図１５】


乱数パラメータ更新処理開始
S211
時間信号を受け取ったか？
No
Yes
S212
乱数パラメータdjを増加
乱数パラメータ更新処理終了

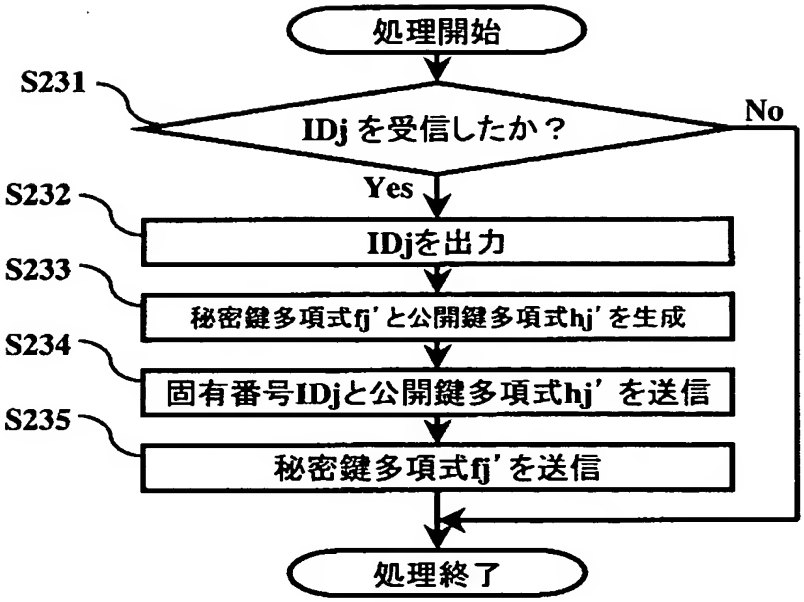
【図１６】


公開鍵更新処理開始
S221
固有番号と新たな公開鍵を受信したか？
No
Yes
S222
DTjを更新
公開鍵更新処理終了

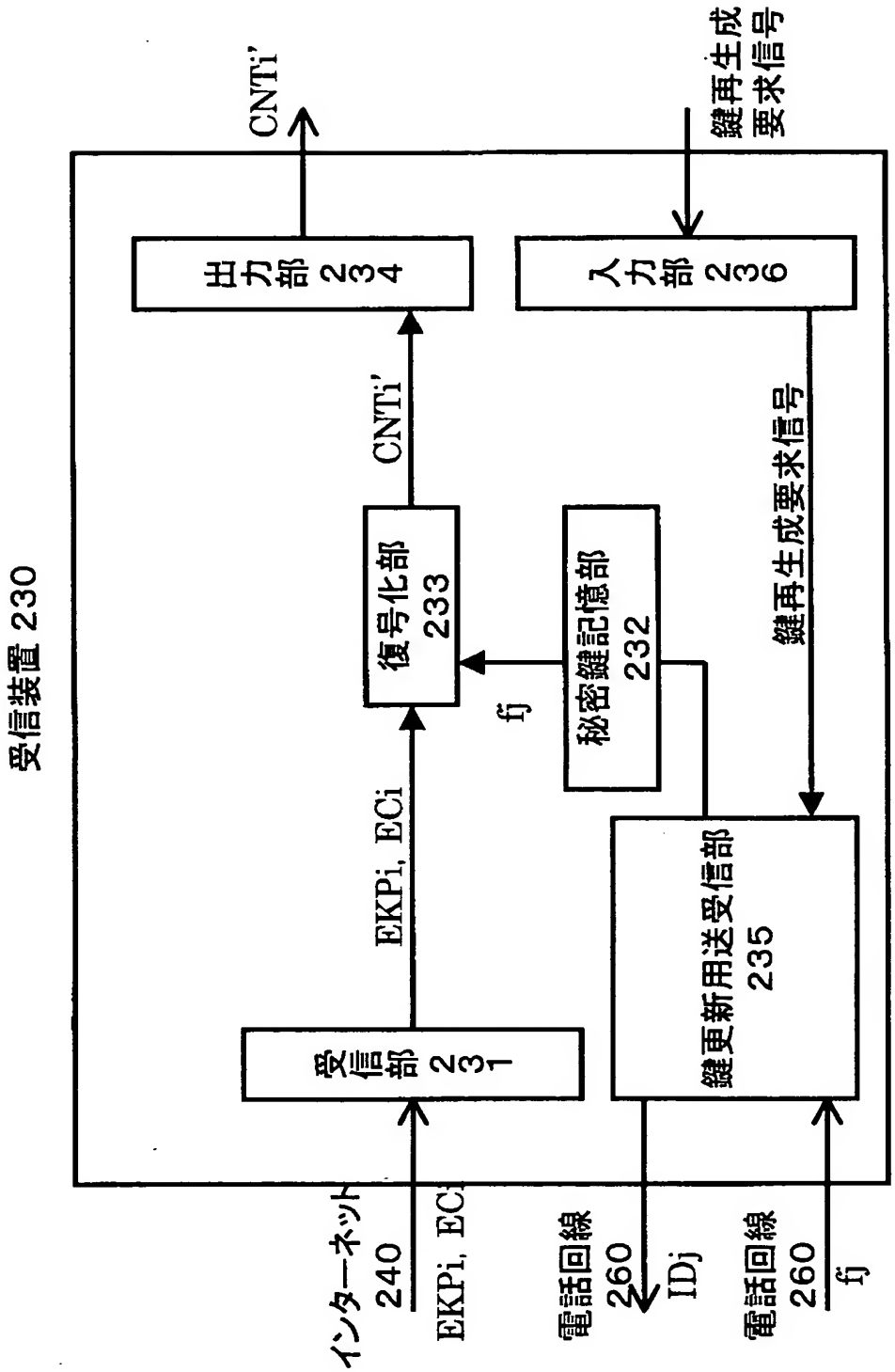
【図１７】


鍵サーバ220
専用回線 250
IDj, hj'
公開鍵送信部 223
IDj, hj'
鍵再生成部 222
fj'
ID受信部 221
秘密鍵送信部 224
電話回線 260
IDj
電話回線 260
fj'

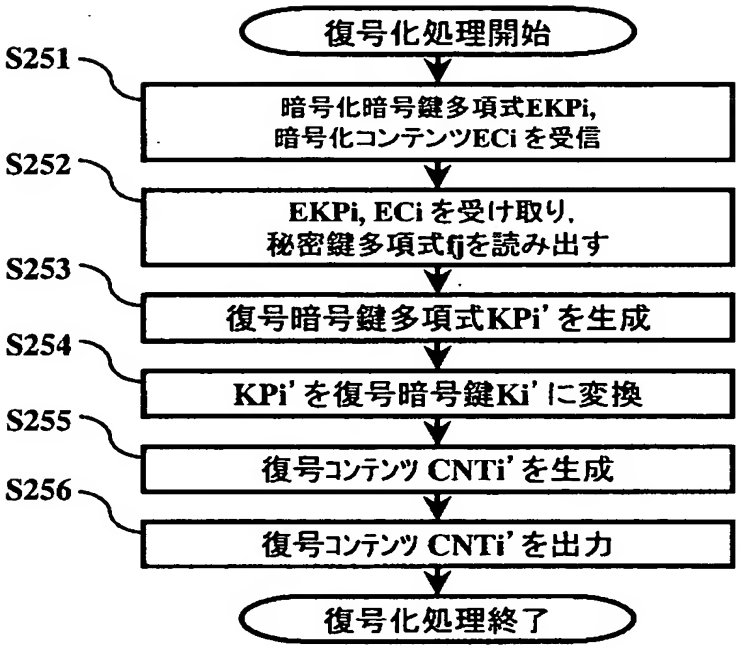
【図１８】


処理開始
S231
IDj を受信したか？
No
Yes
S232
IDjを出力
S233
秘密鍵多項式fj'と公開鍵多項式hj'を生成
S234
固有番号IDjと公開鍵多項式hj' を送信
S235
秘密鍵多項式fj'を送信
処理終了

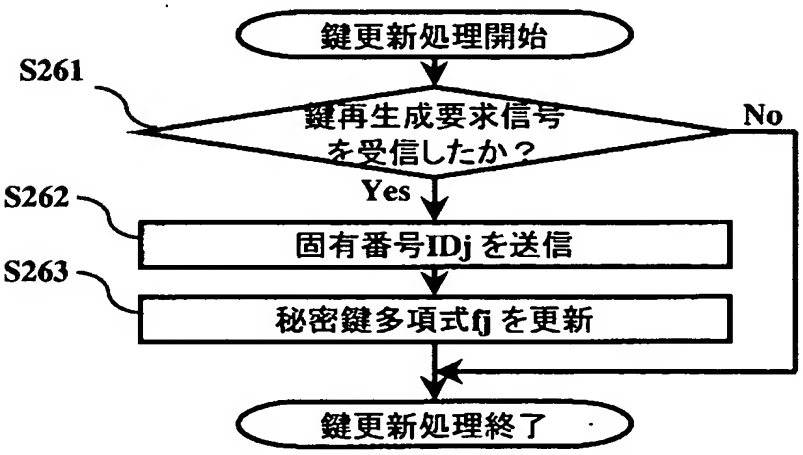
【図１９】


受信装置 230
CNTi'
鍵再生成要求信号
出力部 234
入力部 236
CNTi'
鍵再生成要求信号
復号化部 233
秘密鍵記憶部 232
fj
EKPi, ECi
鍵更新用送受信部 235
受信部 231
インターネット 240
EKPi, ECi
電話回線 260
IDj
電話回線 260
fj

【図２０】


復号化処理開始
S251
暗号化暗号鍵多項式EKPi,
暗号化コンテンツECiを受信
S252
EKPi, ECiを受け取り,
秘密鍵多項式fjを読み出す
S253
復号暗号鍵多項式KPi'を生成
S254
KPi'を復号暗号鍵Ki'に変換
S255
復号コンテンツCNTi'を生成
S256
復号コンテンツCNTi'を出力
復号化処理終了

【図２１】


鍵更新処理開始
S261
鍵再生成要求信号
を受信したか？
No
Yes
S262
固有番号IDjを送信
S263
秘密鍵多項式fjを更新
鍵更新処理終了

【書類名】　要約書

【要約】

【課題】　送信装置が暗号化通信を行うに際して、暴露された秘密鍵を不正に用いる第三者の受信装置は、期間が経過すると暗号化通信が復号できなくなる暗号化システム、送信装置又は受信装置を提供し、これにより秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することを第１の目的とする。

【解決手段】　本発明は、外部から入力された平文を暗号鍵で暗号化した暗号文を受信装置へ送信する送信装置が、前記受信装置毎に乱数パラメータを記憶する記憶手段と、前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備えることを特徴とする。

【選択図】　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社